TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond
Tarkvarateaduse instituut

Eva Maria Veitmaa 155408 IAPB

VEEBIPÕHISTE TESTIDEGA SEOTUD RÜNDED JA TULEMUSTE RIKKUMATUSE TAGAMINE TTÜ SISSEASTUMISTESTI NÄITEL

Bakalaureusetöö

Juhendaja: Sten Mäses
MSc

Tallinn 2018

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Eva Maria Veitmaa

18.05.2018

Annotatsioon

Käesoleva töö peamiseks eesmärgiks on luua eeldus Tallinna Tehnikaülikooli küberkaitse magistriprogrammi sisseastumistesti kaitsesüsteemi realiseerimiseks. Töös on uuritud potentsiaalseid ründeid seoses veebipõhiste teadmiste kontrollidega, võimalikke kaitsemeetmeid ja nende rakendamise otstarbekust TTÜ küberkaitse sisseastumistesti raames. Lähemalt on testitud mõningaid olemasolevaid JavaScripti lahendusi ja analüüsitud silmaliikumisdünaamika kui kaitsemeetme kasutamise võimalikkust.

Töö käigus kinnitati, et silmade liikumise jälgimine on üheks sobivaks kaitsemeetmeks ja jõuti järeldusele, et mõningaid olemasolevaid teeke on võimalik kasutada tulemuste rikkumatuse tagamiseks.

Töös on esitatud ründestsenaariume kajastav ründe-kaitsepuu ja TTÜ küberkaitse sisseastumistesti kaitsesüsteemi kirjeldus ning nõuded.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 51 leheküljel, 8 peatükki, 26 joonist, 7 tabelit.

Abstract

Attacks regarding online tests and ensuring the integrity of results based on the example of TTÜ admission test

The purpose of this thesis is to enable the implementation of an invigilation system as a means to ensure the integrity of results of the entrance exam of cyber security specialty at Tallinn University of Technology by providing the initial analysis. In this study, potential attacks and protective measures regarding online assessments are examined on the basis of the example of TTÜ cyber security admission test. Possible attacks and safety measures are visualized by means of an attack-defence tree. In addition, select JavaScript solutions, such as speech detection and facial recognition using both tracking.js library and Kairos API, are tested as likely components for the invigilation system. From prospective defence measures eye movement dynamics is further analysed using eye tracking hardware by Tobii Pro.

The results of the tests done with eye tracking technology show that dedicated hardware, such as an infrared eye tracker, is a more effective means of following user's gaze point than commercial hardware, for example a web camera. The findings indicate that while mimics may betray what type of web page, for instance YouTube or RangeForce, is being used, the same thing cannot be confirmed by eye movement dynamics only. On the other hand, eye movement can be used to determine whether graphical or text-based content is being viewed. Furthermore, it appears that the order of gaze fixation and mouse movement actions gives sufficient information to verify whether actions are being carried out by the user themselves or simply being viewed, for example by using another monitor. The results also reveal that users combine several methods to enter commands in terminal window, such as typing the text out manually or copying and pasting it using either keyboard shortcuts or a mouse.

While speech recognition API tested in this study is too sensitive to other sounds and can therefore not be utilized in a defence system, satisfying results can be witnessed with both commercial face recognition tools examined. It was also confirmed that an ordinary web

camera can be used for eye tracking, although the results are less accurate than with professional equipment.

Although, as a result of this thesis, the description and requirements of the invigilation system for TTÜ cyber security admission test are given, this study can also be used to implement protective systems for other web based environments where continuous authentication of the user is considered important. It is expected that this work will enable to ensure the integrity of processes that need online interaction.

The thesis is in Estonian and contains 51 pages of text, 8 chapters, 26 figures, 7 tables.

Lühendite ja mõistete sõnastik

Brauser	Ka veebilehitseja, veebisirvija. HTML-dokumentide lugemist võimaldav programm [1].
Buutima	*To boot*. Alglaadima. „Operatsioonisüsteemi arvuti põhimälusse laadima ja käivitama.“ [1]
DevOps	„Koostööd soodustav kultuuriline ja operatiivne mudel, mis tagab IT suure jõudluse ärieesmärkide saavutamiseks.“ [2]
EER	*Equal error rate*, veamäär [3]. Olukord, mil valepositiivsete ja valenegatiivsete väärtuste esinemine on võrdne [4].
Ekraanipilt	*Screenshot*. Kuvariekraanil parasjagu näha oleva visuaalse informatsiooni salvestamise tulem graafikafaili kujul [1].
Elektroentsefalograafia (EEG)	Ajutegevuse mõõtmine, peaaju bioelektrilise aktiivsuse registreerimine läbi naha, kolju ja ajukestade [5], [6].
Elektrokardiograafia (EKG)	Südame elektrilise aktiivuse mõõtmine [3], [6].
Funktsiooniklahv	*Function key*. „Kuum klahv“. Spetsiaalset ülesannet täitvad klahvid arvutiklaviatuuril (F1 kuni F12) [1].
Hoidla	Repositoorium, rakendustarkvara juurde kuuluva info andmebaas [1], [7].
IP-aadress	Internetiaadress, võrgus asuva arvuti või muu seadme identifikaator [1]
Kuvahõive	Arvutiekraanil toimuvast koopia tegemine operatsioonisüsteemi vahendite, rakenduse või välise seadme (nt kaamera) abil, *screen capture* [1].
LFW	*Labeled Faces in the Wild*, kuulsuste fotode andmebaas [8]
LMS	*Learning management system*, veebipõhine õpikeskkond, õppeinfosüsteem. Veebipõhine keskkond, mis võimaldab hallata kursuseid, õppematerjale, õppureid ja tulemusi. [9]
LTI	*Learning Tools Interoperability*, standard õppekeskkondade ja väliste rakenduste ning vahendite ühendamiseks [10]
Matkimisrünne, kehastusrünne	Isiku esinemine kellegi teisena (*impersonation*), identiteedi jagamine [11]. Isik A väidab end olevat isik B.
MOOC	*Massive open online course*, vaba juurdepääsuga e-kursus, tasuta veebipõhine kursus [12], [13]

Muutmälu	Suvapöördusmälu, RAM (*random access memory*). Arvuti keskne mäluseade, millesse salvestatud info kustub toite välja lülitamisel [1].
NIR	*Near infrared*, lähi-infrapunane (valgus) [14], [15].
Plugin	Pistikprogramm, pistik. Suuremale süsteemile teatud omadust või teenust lisav tarkvaramoodul [1].
Pääsmik	*Security token*. „Füüsiline volitustõend, näiteks kiipkaart või USB kaudu ühendatav seadis.“ [16]
Raalnägemine	*Computer vision*. Masina abil ümbritsevast füüsilisest maailmast pärineva visuaalse informatsiooni kogumine ja tõlgendamine [1].
Rakendusliides	Ka API-liides, programmiliides. Rakendusprogrammiga või arvuti operatsioonisüsteemiga määratud reeglistik, mille alusel rakendusprogramm kasutab teise rakendusprogrammi või operatsioonisüsteemi teenuseid [1].
RAM-ketas	Kirjutatav ketas [1].
Ründe-kaitsepuu	Ründe tulemuseni viivate võimalike teede esitus koos ründeid tõrjuvate kaitsemeetmetega [17].
Ründepuu	Ründe tulemuseni viivate võimalike teede formaliseeritud esitus. Nõrkustest võimalike ründetulemusteni viivate teede formaliseeritud esitus. [16]
Spektroskoopia	Aine ja kiirguse interaktsiooni (neeldumine, emissioon, hajumine) uuriv teadusharu [5], [18].
Taasesitusrünne	Andmete salvestamine ja taasesitamine näiteks kasutajatuvastussüsteemi petmiseks [16].
Teek	*Library*. Valmiskompileeritud alamprogrammid ehk moodulid [1].
TTÜ	Tallinna Tehnikaülikool.
Variisik	Isik, kelle nime all tegutseb keegi teine (*impostor*) [19]. Matkimis- ehk kehastusründe ehk identiteedi jagamise läbiviija. Isik A, kes väidab end olevat isik B.
Veebilehitseja	Ka brauser, veebisirvija. HTML-dokumentide lugemist võimaldav programm [1].
Võõrküpsis	*Third party cookie* [20]. Lühike andmeplokk, mille salvestab kasutaja arvutisse mõni muu veebileht kui see, mida hetkel külastatakse [1].
W3C	*World Wide Web Consortium*. Rahvusvahelise Interneti ja veebiga tegelevate firmade konsortsium, mille eesmärgiks on välja töötada avatud standardeid, tagamaks veebi arenemist kindlas suunas [1].

Sisukord

Jooniste loetelu

Tabelite loetelu

1 Sissejuhatus

Haridustee ei eelda tänapäeval enam seotust ülikooli füüsilise asukohaga. Kursuseid ning koguni akadeemilisi kraade on võimalik omandada ka veebipõhiselt oma kodu mugavustest lahkumata. Kuna kodust keskkonda on keerulisem kontrollida, kaasneb veebipõhiste testidega mitmeid eksamikorra rikkumise ohte, nagu näiteks keelatud abimaterjalide kasutamine, kaaslastega konsulteerimine või kehastusrünne ehk olukord, kus testi sooritab tegeliku kandidaadi asemel keegi teine. Seetõttu ongi käesolevas töös kvalitatiivseid meetodeid kasutades uuritud potentsiaalseid ründeid seoses veebipõhiste teadmiste kontrollidega, võimalikke kaitsemeetmeid (sh kasutaja pidevtuvastus) ja nende rakendamise otstarbekust Tallinna Tehnikaülikooli küberkaitse magistriprogrammi sisseastumistesti tulemuste usaldusväärsuse tagamiseks.

Antud töö raames on seatud järgmised eesmärgid:

- testida mõningate kaitsemeetmete realiseerimist võimaldavaid olemasolevaid lahendusi (isikutuvastus, ruumihelist inimkõne eristamine, silmade liikumise jälgimine), muuhulgas pilgu ja hiire liikumise korrelatsiooni ning külastatava veebilehe ja sooritatavate tegevuste määramise võimalust silma fookuspunktide baasil;

- leida sobiv kombinatsioon pidevtuvastuse ja jälgimismeetodite seast, mis takistaks petmist TTÜ küberkaitse eriala sisseastumistestil;

- võimaldada hiljem käesolevale tööle toetudes välja arendada tarkvaralahendus, mille abil suurendada TTÜ küberkaitse eriala sisseastumistesti tulemuste terviklust (*integrity*) ja usaldusväärsust.

Peatükis 2 on esitatud TTÜ sisseastumistesti kirjeldus ning peatükis 3 senised saavutused veebitestide järelevalve valdkonnas. Peatükk 4 keskendub võimalikele rünnetele ja kaitsemeetmetele, millest on mõnd lähemalt katsetatud peatükkides 5 ja 6. Viimaks on kogu eelnevale tööle toetudes peatükis 7 esitatud kaitsesüsteemi kirjeldus.

2 Tallinna Tehnikaülikooli küberkaitse õppekava

Alates 2009. aastast pakub Tallinna Tehnikaülikool tudengitele võimalust õppida küberkaitse magistriõppes [21]. Käesoleva õppekavaversiooni kood on IVCM09/18, maht 120 EAP-d jaotatuna nominaalõppeaja nelja semestri peale ning seda pakutakse koostöös Tartu Ülikooliga [22]. Õppetöö toimub inglise keeles ning sisseastumistingimusteks on muuhulgas varasem kõrgharidus või töökogemus info- ja kommunikatsioonitehnoloogia valdkonnas.

Õppekava eesmärgiks on valmistada tudengeid ette süvaõppeks küberkaitse, digitaalse ekspertiisi või krüptograafia peaerialal ning arendada nii teoreetilisi teadmisi kui ka praktilisi oskusi, tegelemaks infosüsteemide turvalisuse, digitaalsete tõendusmaterjalide ning arvuti turvaintsidentidega [22]. Võimalik on läheneda nii tehnoloogilise, teoreetilise kui ka organisatoorse nurga alt.

Küberkaitse magistriprogrammi sisseastumisprotsessi käigus tuleb Tallinna Tehnikaülikoolile esitada oma Curriculum Vitae ja motivatsioonikiri, sooritada simulatsiooniülesandeid sisaldav veebipõhine sisseastumistest ning läbida vestlus [23].

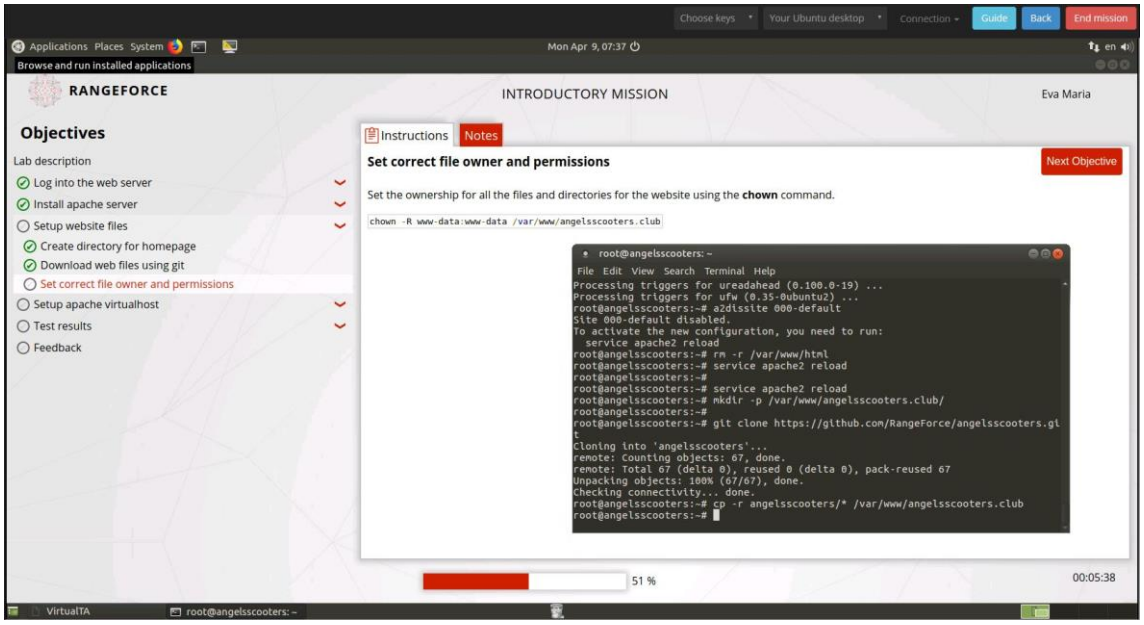
2.1 Sisseastumistesti keskkond

Tallinna Tehnikaülikooli küberkaitse magistriprogrammi tehniline test sooritatakse RangeForce [24] virtuaalses keskkonnas, mis põhineb vabavaralisel i-tee tarkvaral [25]. Tegemist on pilvepõhise platvormiga, mille eesmärgiks on jäljendada tõsielulisi ründestsenaariume, võimaldades küberturbe spetsialistidel, arendajatel ja DevOps valdkonna töötajatel enda oskusi pidevalt proovile panna.

Pärast ülikoolile sisseastumisavalduse esitamist edastatakse kandidaadile unikaalne kood, millega RangeForce keskkonnale ligi pääseb. Sisseastumistest koosneb neljast RangeForce'i virtuaalmasinas sooritatavast missioonist ehk laborist (vt Joonis 1), millest on soovituslik läbida vähemalt üks. Eri laborite lahendamist võib jaotada mitme päeva

peale, kuid kuna hinnatakse ka ülesandele kulunud aega, on soovituslik laborit kord alustades pause mitte teha.

Sisseastumistestil käsiteldavad teemad hõlmavad muuhulgas näiteks Linux CLI, Apache, HTTPS ja SQLi valdkondi. Laborite sooritamise ajal pakub RangeForce keskkond kandidaatidele juhiseid ja näpunäiteid, hõlbustamaks ülesannete lahendamist.



Joonis 1. Kuvapilt RangeForce laborist.

Kuna test on veebipõhine ja selle sooritamiseks ei pea Tallinna Tehnikaülikooli füüsiliselt kohale tulema, kaasneb kandideerimisprotsessil matkimis- ehk kehastusründe (*impersonation*) oht. Nimelt võib avalduse esitanud kandidaat otsustada, et konsulteerib testi tegemise ajal mõne endast targema isikuga või laseb kogunisti terve testi sooritada variisikul ehk kellelgi teisel kui endal. Viimast juhtu ongi antud töös nimetatud ka kehastus- ehk matkimisründeks. Kuna test sooritatakse enne vestlusvooru, on kahtluste esinemise korral võimalik intervjuul testi kohta täpsustavaid kontrollküsimusi esitada.

3 Olemasolevad lahendused veebipõhiste testide rikkumatuse tagamiseks

Alljärgnevalt on välja toodud mõningad lahendused veebipõhise õppe ja eksamite rikkumatuse tagamiseks nii akadeemilises kui kommertsvaldkonnas.

3.1 Akadeemilised uuringud

Fask *et al.* leiavad, et traditsioonilist järelevalvega klassiruumis toimuvat eksamit sooritavatel tudengitel on eelis nende ees, kes teevad testi koduses keskkonnas, kuna viimastel puudub võimalus vaatlejalt täpsustavaid küsimusi küsida ja esineda võib probleeme arvuti või internetiühendusega [26]. Lisaks järeldavad nii Fask *et al.* kui ka Harmon ja Lambrinos [27] oma tulemustest ka seda, et veebipõhistel järelevalveta eksamitel esineb eksamikorra rikkumist (*cheating*) sagedamini. Alessio *et al.* uurimise tulemused viitavad sellele, et järelevalvega veebipõhiste eksamite sooritajate tulemus on halvem kui ilma järelevalveta eksaminandidel [28]. Eksamikorra rikkumist võib vähendada keelatud tegevuste ja nendega kaasnevate tagajärgede kuvamine hoiatusena vahetult enne eksami algust [20]. Sindre ja Vegendla on esile toonud veebipõhistele eksamitele iseloomulikud probleemid: kehastusrünne (*impersonation*), koostöö või kõrvalistelt isikutelt abi saamine, plagiaat, keelatud abimaterjalide (kalkulaator, teatmeteosed) kasutamine, sooritusaja rikkumine (varem alustamine, hiljem lõpetamine), tehniliste probleemide kohta valetamine aja juurde võitmise eesmärgil, eksamiküsimuste salvestamine ja hilisem edastamine teistele eksaminandidele [29].

Bawarith *et al.* kasutavad petmise tuvastamiseks sõrmejäljega sisselogimist, peavad arvet aja üle, mil kandidaat eksami ajal arvutiekraani ees ei viibi ning jälgivad kandidaadi silmade fookuspunkti, välistamaks kaamera vaateväljast eemale jäävate kõrvaliste materjalide kasutamist [30]. Peaasendit ja vastamise ajalist viidet on potentsiaalse petmise vastase kaitsemeetmena uurinud Chuang *et al.* [31].

Rosen ja Carr eksperimenteerivad USB-ga arvuti külge ühenduva kaameraga robotiga, mis filmib suvalise mustri alusel eksamikeskkonda ja arvutiekraani, kuid keskendub vajadusel heliallikale [32]. Nemad kontrollivad eksaminandi identiteeti kõrvatuvastuse alusel [32], samas kui Atoum *et al.* kasutavad sülearvutit, peakaamerat ja mikrofoni, et teha kindlaks kasutaja isik ning tuvastada eksamikeskkonnas kõrvalise teksti, heli ning telefoni olemasolu [33].

Fenu *et al.* keskenduvad veebipõhise õppe puhul kehastusründele ja kasutavad selle vältimiseks multibiomeetrilist pidevtuvastussüsteemi (vt Lisa 2 jaotis 2), mille eesmärk on vältida ülesande- ja seadmespetsiifilisust, see tähendab, et tuvastus töötab erinevat tüüpi ülesannetega (tekstivastus, valikvastus, suuline vastus jm) ja nii süle- ja lauaarvutite kui ka tahvlite ja mobiiltelefonide korral [34]. Nende lahendus kontrollib nägu, häält, puudet, hiirt ja klahvivajutusi, tuvastamaks kasutajat kogu kursuse vältel.

Multimodaalsusele keskenduvad ka Traoré *et al.*, kes soovitavad pidevtuvastuseks kombineerida näotuvastust, hiire kasutusviisi ja trükkimise dünaamikat, põhinedes kasutajal juba olemas oleval riistvaral (veebikaamera, hiir, klaviatuur) [11]. Infot antud biomeetriliste näitajate kohta kogutakse eksami jooksul passiivselt ehk kasutajat häirimata ning lubamatu käitumise (matkimisrünne, eksaminandi lahkumine kaamera vaateväljast, mitu isikut eksamit lahendamas) esinemisel teavitatakse eksami järelevalve teostajat. Nende pakutud raamistik leidis kasutust ExamShield platvormi arenduses.

Clarke *et al.* kaitsesüsteem pakub võimalust kasutajat tuvastada ja jälgida ilma õppesüsteemi tegevusse sekkumiseta [35]. Nende e-Invigilator'i puhul puudub vajadus alla laadida lisatarkvara, kuna tegemist on brauseripõhise lahendusega. Oma töös implementeerisid nad vaid näotuvastuse osa.

Amigud *et al.* keskenduvad kasutaja tuvastamisele sisuloome alusel [36]. Nimelt leitakse, et ühe ja sama tekstilise ülesande lahendamiseks kasutatav kirjutamisstiil, -mustrid ja sõnavara erinevad inimeste lõikes ning nende alusel on võimalik isikut tuvastada. Amigud *et al.* lahendus tuvastas teksti autori 93-protsendilise täpsusega. Võrdluseks, et kursuste juhendajad suutsid tudengite kirjastiili võrreldes pettust avastada vaid 12% juhtudest.

Mothukuri *et al.* on oluliseks pidanud lukustusbrauseri olemasolu (vt Lisa 2 jaotis 5), mis takistab ligipääsu keelatud programmidele ja funktsioonidele, ja näo- ning hääletuvastuse rakendamist, tuvastamaks ruumis esinevaid kõrvalisi isikuid [37].

Carlisle ja Baird pakuvad välja spetsiaalse CD-lt buutiva lukustussüsteemi, milles on asendatud tavapärane failide avamise ja sulgemise dialoogaken [38]. Failid salvestatakse krüpteeritult kasutaja arvuti kõvakettale, millele testi sooritamise ajal ligi ei pääse, ja krüpteerimata kujul RAM-kettale, kust kasutaja neid avada saab. Blokeeritud on võrguühendus, USB-pesad, paremklikk ja kuigi lukustussüsteemi saab jooksutada virtuaalmasinas, märgistatakse sellisel juhul salvestatud failid ning neid ei krüpteerita. Väliselt kettalt buutivat autentimisvõtmega testsüsteemi soovitavad ka Rosen ja Carr [32].

Mõningad teaduslikud uuringud on näidetena eraldi välja toodud ka vastavate kaitsemeetmete juures (vt Lisa 2).

3.2 Kommertslahendused

Eksisteerivad laiatarbelised eksami järelevalve lahendused jagunevad üldpildis neljaks.

Kõige traditsioonilisem neist on eksami sooritamine kontrollitud keskkonnas, nagu eksamikeskus või eraldatud ruum ülikoolis. Testi tegemise ajal jälgivad kandidaate vaatlejad, kelle ülesandeks on tuvastada ebaausat käitumist, nagu kaaslasega konsulteerimine, spikerdamine või keelatud abivahendite kasutamine. Kui vaatlejateks on enamasti sama asutuse töötajad, võib kindel olla, et nad on kursis spetsiifiliste reeglitega, mida asutus eksamite korral rakendab, nagu lubatud abivahendid. Kahjuks aga ei suuda ülikoolid enamasti palgata piisaval hulgal vaatlejaid, et tuvastada kõik ebaausa käitumise katsed. Veebipõhiste kursuste korral muudaks kohustus füüsiliselt eksamikeskusesse tulla eksaminandide elu keerulisemaks ja MOOCide ehk vaba juurdepääsuga e-kursuste puhul oleks taoline nõue osalejate suurest arvust ja vahemaast tulenevalt mõeldamatu.

Reaalajas võrgujärelevalve korral kontrollitakse kandidaati kogu testi lahendamise vältel. Vaatluse all on nii ekraanil toimuv kui ka eksami sooritaja ise näiteks ekraanijagamistarkvara, mikrofoni ja veebikaamera pildi vahendusel [39]. Järelevalvet teostab ideaalis isik, kes on läbinud vastava koolituse ja oskab tähele panna petmisele viitavaid märke. Kuigi taoline lahendus võimaldab eksamit sooritada asukohast sõltumatult, eeldab see siiski ühise aja kokku leppimist ja sobiva kvalifikatsiooniga vaatleja palkamist ning on sellest tulenevalt majanduslikult kulukas ja raskesti vajadusele kohandatav, kuna üks vaatleja suudab korraga jälgida vaid piiratud arvul õpilasi [40]. Ka

siin ei pruugi vaatleja märgata kõiki rikkumisi, kuid kuna kandidaat ei tea, millisel ajahetkel just teda jälgitakse, võib väheneda soov petta. Mõned firmad pakuvad eksami järelevalve teenust koos enda poolsete vaatlejatega, kuid erinevalt kohaliku akadeemilise personali protsessi kaasamisest ei saa firmade puhul kindel olla, et vaatlejad on usaldusväärsed ja kursis konkreetse asutuse eksamireeglistiku ja akadeemiliste tavadega. Reaalajas võrgujärelevalvet pakub näiteks Pearson VUE [41].

Salvestatava järelevalve puhul lindistatakse heli- ja videoseadme abil eksaminandi ennast ja tema arvutiekraanil olevat pilti, mida vaatleja hiljem mitmekordsel kiirendusel kontrollib, et analüüsida hetki, mil võis aset leida pettus [42]. Kuigi antud lahendus ei nõua, et eksami sooritamine ja järelevalve toimuksid samaaegselt, ning võimaldab sooritust vaadata tempokamalt kui reaalajas, on kontroll siiski jätkuvalt seotud inimfaktoriga, mille usaldusväärsuses ei saa kindel olla juhul, kui tegemist pole vastavalt kvalifitseeritud personaliga. Samuti tekib viivitus eksamitulemuste teada saamisel, kuna eelnevalt tuleb kindlaks teha, et tudeng ei ole reegleid rikkunud. Positiivse poole pealt säilib eksamist digitaalne tõend, mis hõlbustab hilisemate apellatsioonide lahendamist. Antud valdkonnas on pikalt tegutsenud Software Secure firma [43].

Automaatne järelevalve eeldab sarnaselt eelnevatele ekraani ja kandidaadi lindistamist, kuid lisaks sellele analüüsib süsteem jooksvalt heli ja videopildi andmevoogu, tuvastamaks kahtlustäratavat ja ebasobivat käitumist [42]. Erinevate algoritmide abil kontrollitakse ruumi valgustust, kaadris asuvaid kahtlaseid objekte, eksamineeritava keskendumist ekraanile, taustaheli ja -pilti. Näotuvastus kindlustab, et testi sooritab üks ja sama isik. Ohukohad märgistatakse ning kuigi teoreetiliselt peaks kogu järelevalvega hakkama saama automaatsüsteem, on neid soovi korral võimalik hiljem ise üle kontrollida. Inimesest vaatleja puudumine tähendab, et ei eksisteeri piirangut eksami sooritamise ajale ja kohale, ning kogu süsteem muutub paremini vajadusele kohandatavaks, võimaldades kandidaatidele seada lisatingimusi näiteks piiratud operatsioonide või teiste rakenduste avamise takistamise näol. Kõiki kandidaate koheldakse võrdselt, sest vaatlejaks on algoritm, mitte inimene. Soovi korral on eksaminande ka testi sooritamise ajal võimalik teavitada potentsiaalsest rikkumisest, tuletamaks meelde reeglistikku ja võimaldamaks selle alusel käitumist parandada. Kahjuks ei ole olemasolevad automaatsed järelevalvesüsteemid veel piisavalt head, et osutuda majanduslikult kasumlikuks. Mõned olukorrad märgitakse valepositiivselt ning mõned tagasihoidlikumad spikerdamiskatsed jäävad arvutil märkamata, mis tähendab, et

lõpliku kontrolli peab jätkuvalt teostama inimene. Ühe Software Secure kliendi puhul märgiti 100 000-st toimunud eksamist potentsiaalseid pettuseid sisaldavaks 2425, millest reaalne rikkumine toimus 613 eksamil [40]. See tähendab, et algoritm tuvastas rikkumisi vääralt 75% juhtudest. Samuti ei saa automaatset eksamijärelevalvet kasutada, kui lubatud on abimaterjalid, sest süsteem ei tee vahet õpikul ja muudel märkmetel. Täisautomaatse järelevalvega testimist pakub firma Talview [44].

Nagu näha, eksisteerib mitmeid erinevaid eksami järelevalveks loodud süsteeme, millest mõned eeldavad lisariistvara olemasolu või nõuavad suuremal määral inimese osalust (vt Tabel 1). Seetõttu saab väita, et turul on juba lai valik kommertslahendusi, mille seast on võimalik endale sobivaim leida, selle asemel, et seda ise luua.

Tabel 1. Järelevalve kommertslahenduste võrdlus.

Lahendus	**Kandidaadi jälgimine**	**Ekraanipildi jälgimine**	**Vajalik lisaseade**	**Integreeritav olemasoleva keskkonnaga**	**Vajalik inimvaatleja olemasolu**
Talview Remote Proctor	x	x		x	
Remote Proctor PRO	(väline lisaseade)	(väline lisaseade)	x	x	x
RPNow	x	x		x	x
Pearson VUE	x	x			x

Igast eelpool mainitud kategooriast on vähemalt üht järelevalvelahendust kirjeldatud lisas 1.

4 Ründe-kaitsepuu

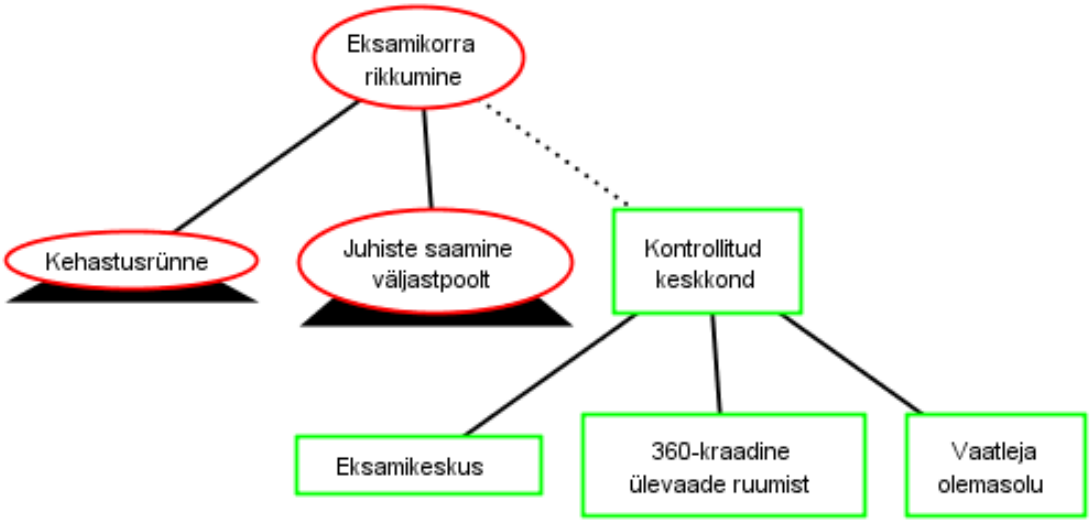
Võimalikke ründeid RangeForce keskkonnas ja kaitseid rünnete vastu on käesolevas töös kirjeldatud ründe-kaitsepuu (*attack-defence tree*) abil. Ründe-kaitsepuu on edasiarendus ründepuust (*attack tree*), mida on defineeritud kui ründe tulemuseni viivate teede formaliseeritud esitust (näiteks graafi või puu kujul) [16]. Ründepuu puhul tähistab puu juur (*root*) ründaja lõppeesmärki (*goal*), iga tipu ehk sõlme (*node*) järglased (*descendant*) viitavad alameesmärkidele (*sub-goal*), mis on tolles sõlmes oleva ründe läbi viimiseks vaja saavutada, ning puu järglasteta sõlmed ehk lehed (*leaves*) kirjeldavad ründaja tegevusi [45]. Ründepuu on väga hea meetod süsteemi turvalisuse analüüsimiseks, kuid erinevalt ründe-kaitsepuust ei võta ta arvesse võimalikke kaitsemeetmeid rünnete takistamiseks ning nende mõju rünnetele.

Ründe-kaitsepuus lisatud kaitsemeetmed võimaldavad jälgida ründaja ja süsteemi kaitsja vahelist suhet ning selle arengut [17]. Ründe-kaitsepuu koosneb kaht liiki sõlmedest: ründe- ja kaitsesõlmed. Igal tipul võib sarnaselt ründepuule olla üks või mitu sama liiki järglast ehk alameesmärki. Lisaks võib sõlmel olla ka üks vastasliiki järglane ehk vastumeede. Niisiis võib ühel ründetipul järglasteks olla mitu rünnet defineerivat sõlme ning üks kaitsemeetme sõlm, mille järglasteks võib omakorda olla mitu kaitset kirjeldavat tippu ning üks ründesõlm, mis vastava kaitse nurjab. Tipu järglaste vahelised seosed võivad olla disjunktiivsed, mille puhul sõlme eesmärk saavutatakse vähemalt ühe sama tüüpi järglase eesmärgi saavutamisel, või konjunktiivsed, mille korral sõlme eesmärk saavutatakse kõigi samaliigiliste järglaste eesmärkide saavutamisel. Kaitse-ründepuud võib vaadelda kui mängu või võistlust ründaja ja süsteemi kaitsja vahel.

Käesolevas töös on ründe-kaitsepuu loomisel kasutatud ADTool tarkvara versiooni 2.2.2 [46]. Ründe-kaitsepuu on oma suurusest tulenevalt esitatud mitme joonise peale jaotatult. Punased ovaalsed tipud tähistavad ründeid ja rohelised nelinurgad kaitsemeetmeid. Joonisel tipu kohal asuv must kolmnurk viitab tipu vanemale ning tipu all asuv must riba tipu lastele, mis on joonisel peidetud. Kaht eriliigilist sõlme ühendab

katkendjoon ning samaliigilisi sõlmi pidevjoon. Antud peatükk keskendub peamiselt potentsiaalsetele rünnetele, kaitsemeetmeid on laiemalt kirjeldatud lisas 2.

RangeForce keskkonnas sisseastumistesti sooritamine jaguneb eksamikorra rikkumise valdkonnas üldpildis kaheks (vt Joonis 2). Üheks ohuks on kehastusrünne ehk olukord, kus kandidaat laseb sisseastumistesti osaliselt või kogu ulatuses sooritada variisikul ehk kellelgi teisel kui ta ise, kuid võimalik on ka välise abi kasutamine ülesande lahendamist hõlbustavate juhiste saamiseks.



Joonis 2. Eksamikorra rikkumise ründe-kaitsepuu.

Mõlema ründe esinemise ohtu aitaks vältida või vähemalt vähendada testi sooritamine kontrollitud järelevalvega ruumis, nagu näiteks eksamikeskus, kus on võimalik veenduda, et seintel ja laudadel pole keelatud lisamaterjale nagu valemid või spikrid, valgustus on sobiv, eksaminandid istuvad üksteisest piisavalt kaugel ja saavad segamatult töötada (vt Lisa 2 jaotis 1). Kodustes tingimustes sooritatava eksami (nagu küberkaitse eriala sisseastumistest) korral on täielikult kontrollitud keskkonna loomine keeruline, kui mitte võimatu, kuid osaliselt kontrollitud keskkonda võib tekitada ka virtuaaleksamitel, kasutades selleks näiteks arvutiekraanist ning ruumist 360-kraadi ulatuses videopilti edastavat kaamerat.

4.1 Kehastusrünne

Kehastusründe kaitsemeetmeks oleks isikutuvastuse rakendamine. Isiku tuvastamine ehk autentimine jaguneb kaheks. Üheks protsessiks on isiku identifitseerimine ehk esitatavate

andmete võrdlemine iga andmebaasis oleva isiku andmetega, leidmaks esitatud andmetele vastavat isikut [47]. Antud juhul on tegemist üks-mitu (1:N) seosega, kus ühe komplekti esitatud andmete puhul käiakse läbi mitu isikut, kuni leitakse vaste.

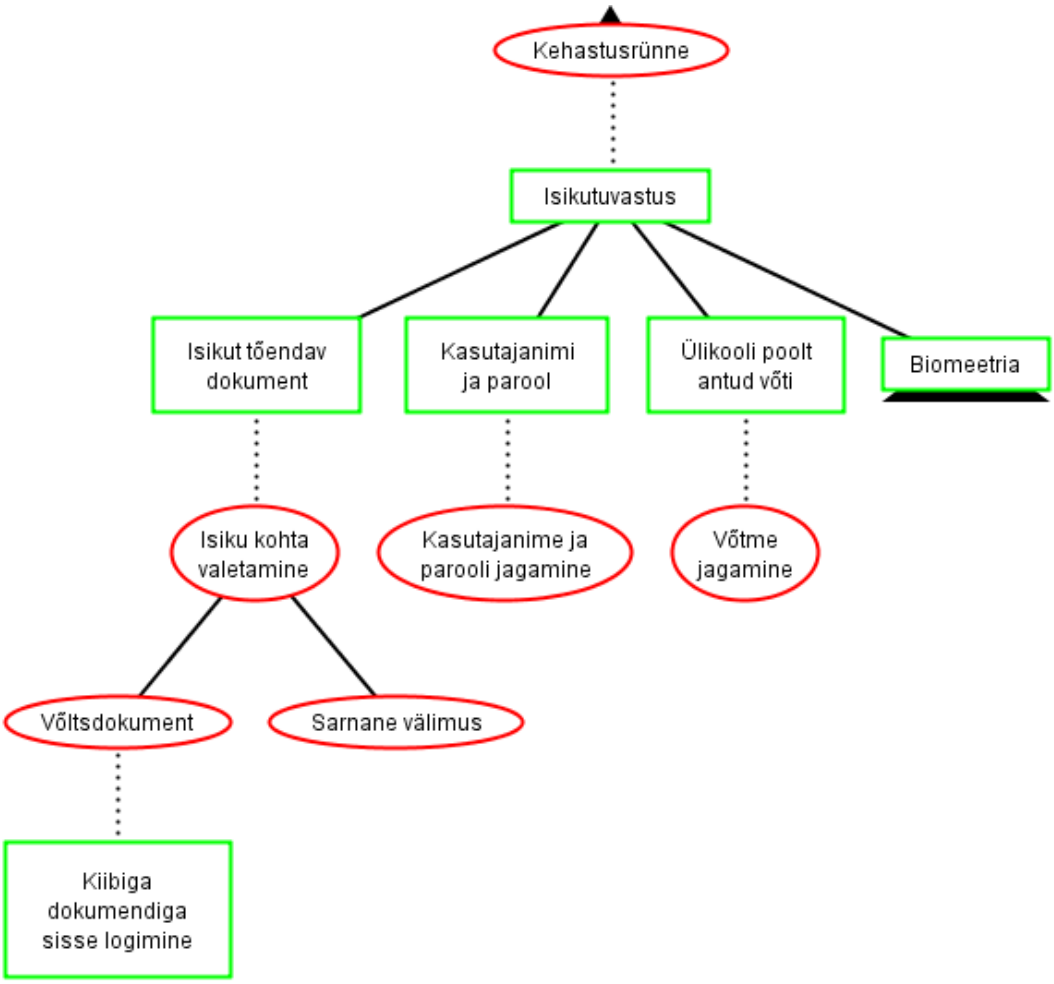
Teine protsess on isiku verifitseerimine, mille käigus üritatakse aru saada, kas andmed esitav isik on see, keda ta väidab end olevat [48]. Sellisel juhul võrreldakse isiku esitatud parameetreid konkreetse andmebaasis oleva isiku andmetega ehk teostatakse üks-üks (1:1) võrdlus. Tulemuseks on tõeväärtus vastavalt sellele, kas esitatud parameetrid vastavad andmebaasis sama isiku kohta käivatele varasemalt teada olevatele parameetritele või mitte.

Eelnevast tulenevalt võib autentimist ehk kasutaja tuvastamist defineerida kui õigel ajahetkel õigete privileegidega õigele isikule õige ligipääsu võimaldamist [47].

Autentimist võib jaotada selle alusel, milliste faktorite järgi isikut tuvastatakse. Selleks võib olla midagi, mida kasutaja teab (salasõna, PIN-kood, turvaküsimuse vastus), mida kasutaja omab (ID-kaart, kiipkaart) või mis iseloomustab kasutajat ennast ehk biomeetria [37], [49], kusjuures viimane jaguneb veel omakorda füüsiliseks (nägu, sõrmejälg, silmaiiris) ja käitumuslikuks (trükkimisstiil, allkiri, kõnnak) biomeetriaks [50] (vt Joonis 4). Kui füüsiline biomeetria on enamasti püsiv ilma kehamodifikatsioone rakendamata, siis käitumine võib aja jooksul muutuda kasvõi kogemuste kogunemise ja süsteemiga harjumise [51], väsimuse või asendi [52] tõttu. Turvalisem on loomulikult mitme teguri kombinatsiooni nõudmine ehk multimodaalne süsteem.

Küberturvalisuse sisseastumistesti arvesse võttes võiks isiku tuvastamiseks kaaluda nelja varianti (vt Joonis 3, lk 24). Üheks neist oleks eksaminandi isiku kindlaks tegemine ametliku isikut tõendava dokumendi abil. Selleks võib kõrvutada dokumendifotot ja kandidaadi nägu. Antud meetod töötaks nii näost-näkku kohtumisel kui ka veebipõhise testi puhul, paludes viimasel juhul dokument kas sisse skannida või fotojäädvustuse tegemise eesmärgil veebikaamera ees hoida. Küll aga ei ole kumbki kaitstud dokumendi võltsimise vastu. Videokaadrist või skannitud fotolt on raske hästi järele tehtud riikliku dokumendi ehtsust kontrollida, eriti ainult visuaalse vaatluse käigus. Eesti näiteks pakub sellele osalist lahendust kiibiga varustatud ID-kaardiga sisse logimise näol.

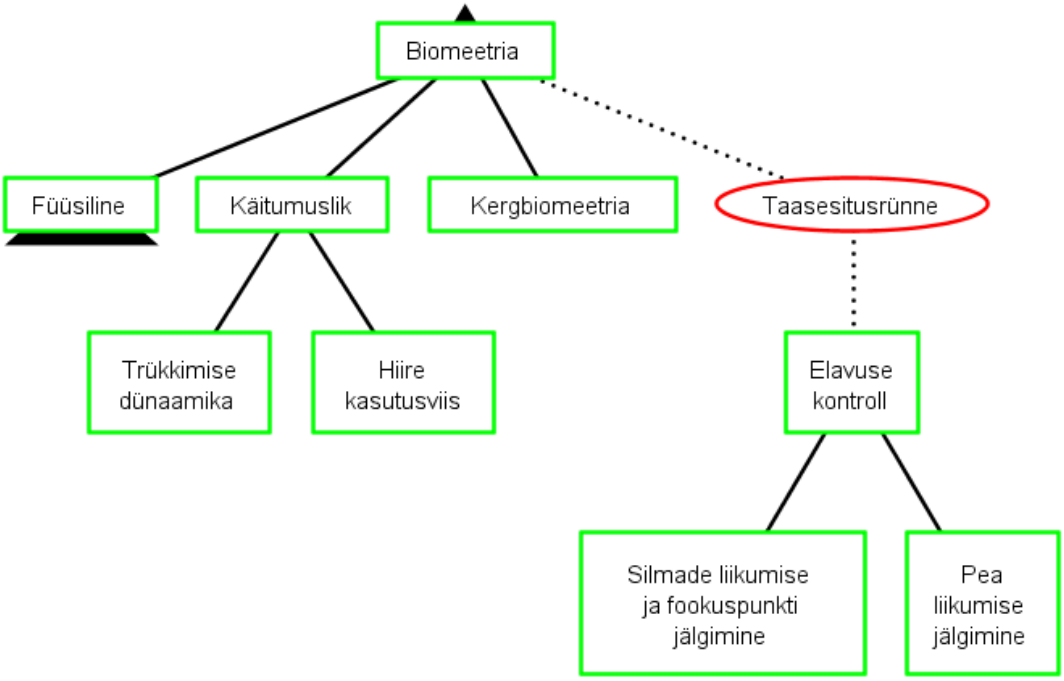
Lisaks võltsdokumendi esitamisele saab isikut tõendava dokumendiga kandidaati tuvastades pettust sooritada ka siis, kui variisik ja tegelik kandidaat on välimuselt sarnased (vt Joonis 3). Selline olukord võib tekkida näiteks ühe munaraku mitmikute korral või välimust abivahenditega (meik, parukas, võltsnäokarvad) muutes.



Joonis 3. Isikutuvastus ja võimalikud ründed.

Teiseks isiku tuvastamise meetmeks oleks paluda kasutajal sisse logida millegagi, mida ta teab või millegagi, mida ta omab (vt Joonis 3). Eksaminandi enda seadistatud kasutajanimi ja hästi valitud parool (ka salasõna) võib olla kaitseks juhul, kui konto omanik ei soovi, et keegi sellele ligi pääseks, kuid sisseastumistesti puhul kehastusrünnet läbi viies võib kandidaat oma isikuga seotud autentimisinfot meelsasti variisikuga jagada. Sama kehtib ka siis, kui ülikool saadaks igale sisseastujale teda identifitseeriva unikaalse võtme või pääsmiku (näiteks kiipkaart või USB-ga ühendatav seade), millega kasutajat tuvastada.

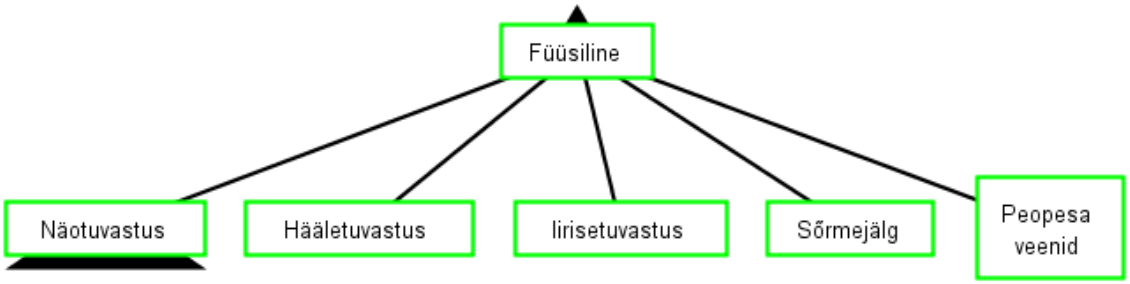
Biomeetriat kui kasutaja tuvastamist tema olemuse järgi saab omakorda jaotada füüsiliseks, käitumuslikuks ning kergbiomeetriaks (vt Joonis 4). Kõik need on tundlikud taasesitusründele (*replay attack*). See tähendab, et biomeetrilisi näitajaid on võimalik mingil kujul (video, foto, helilindistus, sõrmejälg jmt) salvestada ja kopeerida originaalkasutajat jälgides või lindistades. Kui võltsitud karakteristikuid hiljem uuesti tuvastussüsteemile esitades saavutatakse keskkonnale ligipääs, ongi tegemist taasesitusründega. Selle vältimiseks tuleks kontrollida süsteemile esitatava biomeetrilise karakteristiku elavust, näiteks peaasendi või silmade fookuspunkti reageerimist ekraanil kuvatavale stiimulile (vt Lisa 2 jaotis 3) või kehasoojuse ja muude elavusnäitajate, nagu pulss ja elektrijuhtivus, esinemist.



Joonis 4. Biomeetria jagunemine.

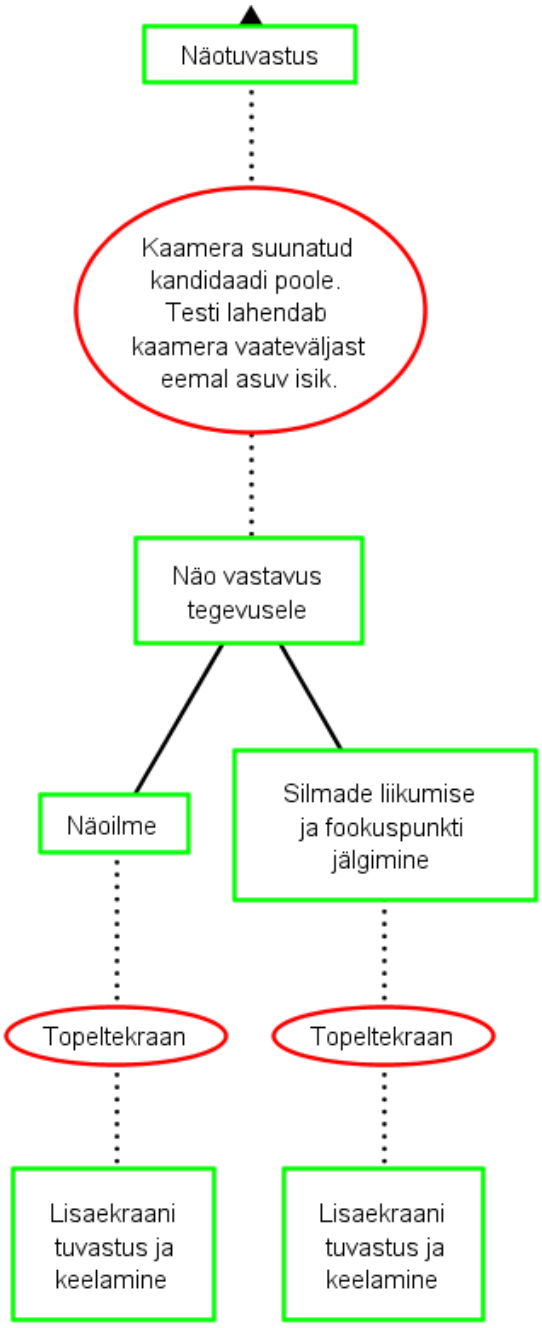
Isikutuvastuseks saab kasutada füüsilisi ja käitumuslikke karakteristikuid, nagu näiteks kasutaja nägu, hääl, silmaiiris, sõrmejälg, peopesa veenimuster (vt Joonis 5, lk 26) või trükkimise dünaamika ja hiire kasutusviis (vt Joonis 4). Neid võib omakorda toetada kergbiomeetriaga, mis põhineb inimkeha eristatavate, kuid mitte individualiseerivate tunnuste (sugu, juuksevärv, riidevärv, armid jmt) võrdlemises [16]. Nendest kõige lihtsam on taasesitada kergbiomeetriat. Selleks võivad variisik ja tegelik kandidaat kanda ühte tooni riideid, parukat või meiki. Kõige keerulisem on täpselt jäljendada käitumist. Sageli ei pööra kasutaja ise teadlikult oma tegevusstiilile tähelepanu, mistõttu vajab

käitumusliku biomeetria taasesitamine teise inimese poolt põhjalikku jälgimist, lindistamist ja selgeks õppimist. Kõiki eelpool mainitud biomeetrilisi näitajaid on lähemalt kirjeldatud töö lisa 2 jaotises 2.



Joonis 5. Füüsilise biomeetria kaitsemeetmed.

Füüsilise biomeetria baasil isiku autentimine on tõenäoliselt kõige lihtsam näotuvastuse abil, kuna seda saab teostada ka tavalist veebikaamerat kasutades. Nõudes kandidaadilt testi sooritamist veebikaamera ees, on kogu protsessi jooksul võimalik jälgida tema nägu ning teha kindlaks isiku vahetumine. Samas võib tekkida olukord, kus näotuvastust teostav kaamera on suunatud kandidaadi poole, kuid selle vaateväljast eemal lahendab sisseastumistesti sellegipoolest variisik (vt Joonis 6). Kuna inimese näoilme kipub sisseastumistesti sooritades ja YouTube'ist videoid vaadates erinema, võiks miimika jälgimine anda vihjeid selle kohta, kas näotuvastuse subjekt tegeleb parasjagu ülesande lahendamisega või mitte.



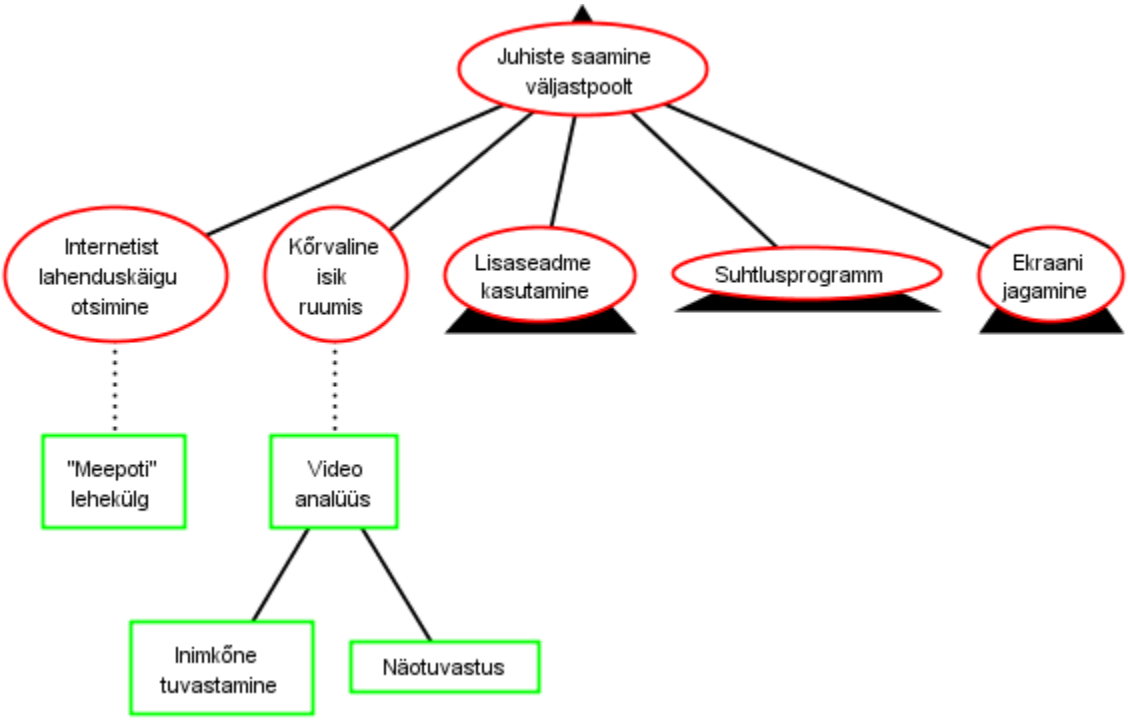
Joonis 6. Näotuvastusega kaasnevad ründed ja kaitsed nende vastu.

Ka silmade liikumise ja fookuspunkti vastavus kursori liikumisele, ekraanile tekkivatele elemenditele ja testis toimuvale võib anda vihjeid selle kohta, kas kaamera ees viibiv isik on testi lahendamas ise või jälgib sooritust lisaekraani vahendusel (vt Joonis 6 ja Lisa 2 jaotis 3). Eeldatavasti vaatab tegevust ise sooritav isik esmalt silmadega nupule, mida vajutada soovib, ning alles pärast silmadega nupule keskendumist liigutab sinna ka kursori. Kuna lisaekraanilt toimuvat jälgiv isik ei tea, mida tegelik testi sooritaja teha kavatseb, tekib pilgu ja hiireliikumise vahel ebakõla. Et vähendada näoilme ja

fookuspunkti abil näotuvastussüsteemi petmist, tasub lisaekraani kasutamine keelata (vt Lisa 2 jaotis 4).

4.2 Välise abi kasutamine

Kuigi küberkaitse sisseastumistest on mõeldud iseseisvaks lahendamiseks, puudub hetkel kontroll selle üle, kas kandidaat leiab lahenduskäigud omapead või kasutab selleks välist abi, näiteks otsib sisseastumistesti täielikku lahenduskäiku internetist[1], kasutades selleks lisaseadet või sama arvutit, millega eksamit sooritab, konsulteerib ruumis või eemal viibiva kõrvalise isikuga vahetult või suhtlusprogrammi abil või kasutab ülesande edastamiseks ja lahendatud saamiseks ekraanijagamisprogrammi abi (vt Joonis 7).

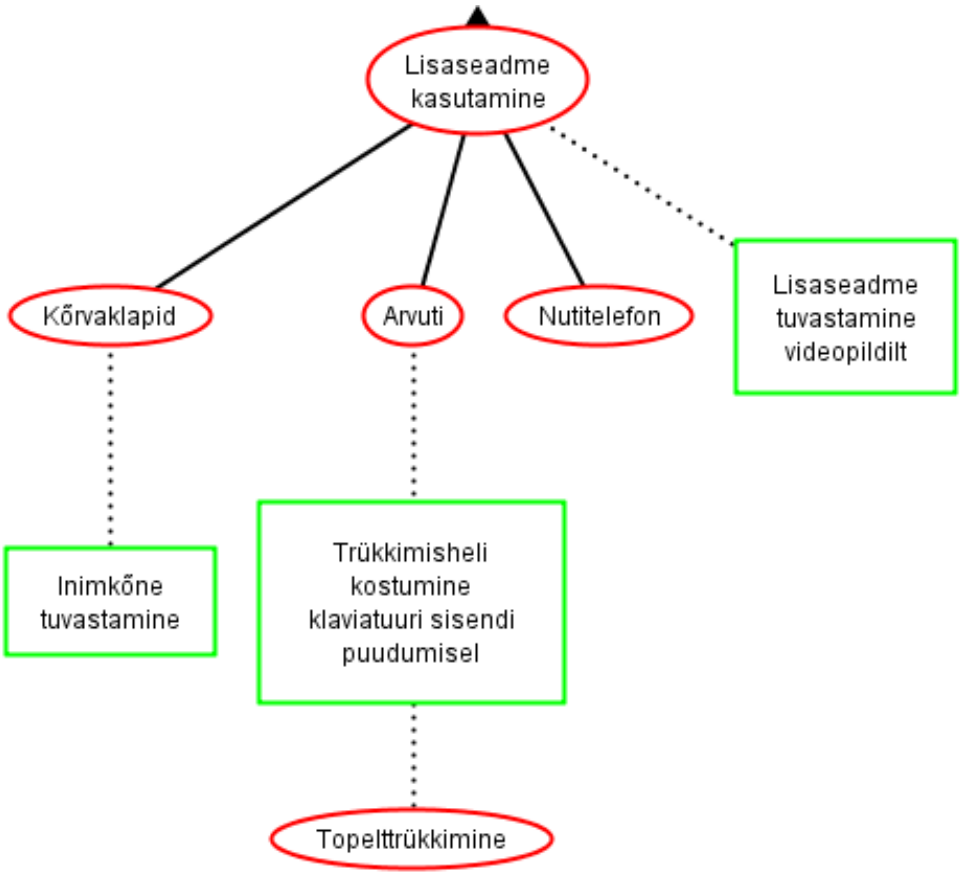


Joonis 7. Välise abi saamine.

Lisaseadme all on mõeldud kellegi teise edastatavate juhiste kuulamist (juhtmevabade) kõrvaklappide abil ja mobiili või teise arvuti kasutamist sisseastumistesti lahenduskäigu otsimise või juhiste saamise eesmärgil (vt Joonis 8). Kuna testi lahendamiseks kasutatava arvuti kaitsesüsteem ei laiene teistele ruumis viibivatele seadmetele, on ainsaks

[1] Alamülesannete lahendamiseks tarvilikke terminalikäske ja teooriat on TTÜ küberkaitse sisseastumiseksami puhul lubatud internetist otsida, aga tervikliku lahenduskäigu kirjelduse järgi testi tegemine langeb eksamikorra rikkumise alla.

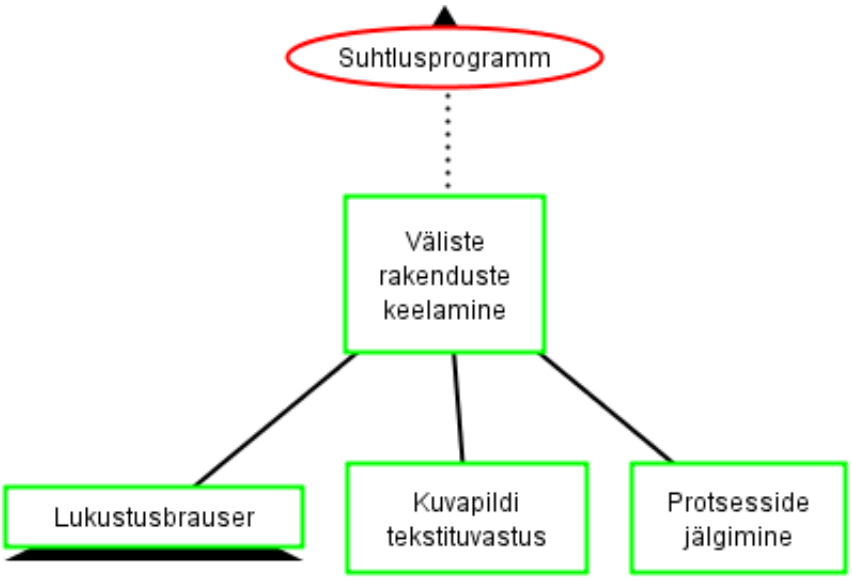
võimaluseks nende tuvastamine heli- ja videopildi kaasabil (vt Lisa 2 jaotised 6 ja 7). Näiteks kõrvaklappide abil juhiseid saades võib esineda hetk, kus kandidaat palub suuliselt juhist täpsustada. Tol hetkel saab ruumi heli kuulates tuvastada inimkõne esinemist, mis võib viidata eksamikorra rikkumisele.



Joonis 8. Võimalikud lisaseadmed ja meetmed nende tuvastamiseks.

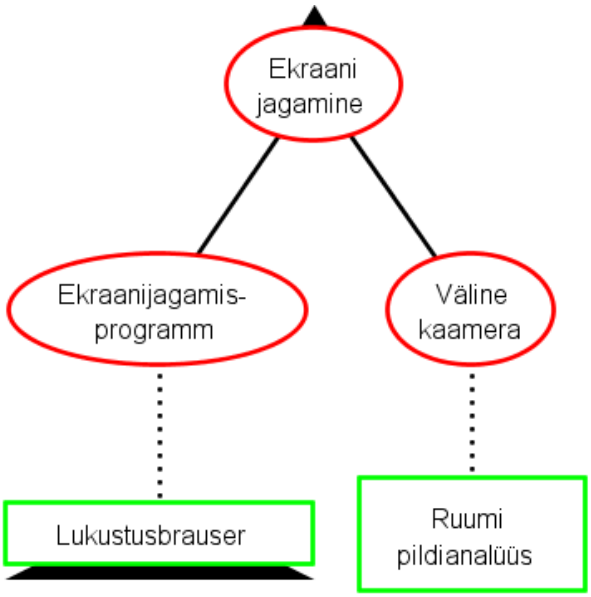
Klaviatuuriga lisaseadet kasutades on ruumis kosta trükkimisheli, kuid puudub sisend arvutil, milles testi sooritatakse. Seda saaks omakorda rünnata, trükkides samaaegselt ka testimismasinal. Sellise olukorra avastamine on juba keerulisem, aga võimalik, näiteks analüüsides, kas konsooli kirjutatud tekst oli lihtsalt suvaliste tähtmärkide jada, mis hiljem ilma käivitamata kustutati, või mitte. Puutetundlike vahendite korral mehaanilisele klaviatuurile spetsiifiline trükkimisheli puudub.

Juhtnööride edastamiseks saab kasutada ka suhtlusprogramme (vt Joonis 9). Selleks on oluline blokeerida ülesandesse mitte puutuvate rakenduste kasutamist ja kõrvaliste veebilehekülgede külastamist (vt Lisa 2 jaotis 5).



Joonis 9. Kaitsed suhtlusprogrammi kasutamise takistamiseks.

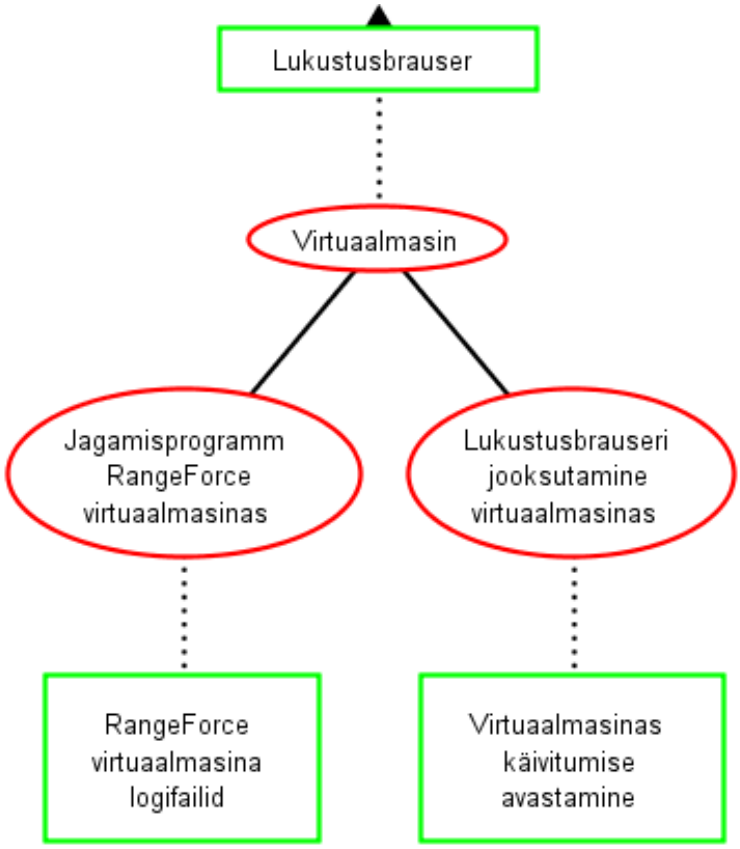
Välise lisakaamera abil on võimalik edastada videopilti arvutiekraanil toimuvast, et selle baasil kelleltki teiselt juhiseid saada (vt Joonis 10). Ekraanijagamisprogrammid võimaldavad lisaks ekraanist reaalajas video edastamisele arvutis toimuvat lausa teisest seadmest juhtida. Koos näotuvastuse kaitsemeetmega sarnaneb see rünne lisaekraani kasutamisele, kuid on ennetatav, kasutades lukustusbrauserit ehk programmi, mis takistab kasutajal teiste rakenduste avamist (vt Lisa 2 jaotis 5).



Joonis 10. Ekraani jagamise rünne.

Siiski pole ka lukustusbrauseri kasutamine ideaalne kaitsemeede, kuna ei takista välise lisaseadme kasutamist, suhtlus- ja ekraanijagamisrakenduste alla laadimist ja käivitamist

RangeForce virtuaalmasinas ning olukorda, kus lukustusprogramm käivitatakse lokaalses masinas jooksma pandud virtuaalmasinas (vt Joonis 11). Viimase puhul on kõrvalised rakendused blokeeritud virtuaalmasinas, aga lokaalses masinas, milles virtuaalmasin käivitati, saab kõiki rakendusi sellest hoolimata kasutada. Seetõttu on oluline tuvastada, kui lukustusbrauser töötab virtuaalkeskkonnas. RangeForce keskkonna siseste toimingute puhul saab keelatud tegevuste avastamiseks kasutada logifaile.



Joonis 11. Lukustusbrauseri kasutamisega kaasnevad ohud.

Nagu eelnevast näha, on võimalusi eksamikorra rikkumiseks hulgaliselt. Lisas 2 on lähemalt vaadeldud võimalikke kaitsemeetmeid RangeForce keskkonnas toimuva sisseastumistesti rünnete ennetamiseks ja tuvastamiseks. Selleks, et teha kindlaks, RangeForce keskkonnas domineerivad ründed, on tulevikus vajalik täiendav uurimine ja kasutajakäitumise analüüs sisseastumistesti sooritamise ajal. Antud töö skoopi arvesse võttes pole neid käesolevas töös käsitletud.

5 Silmaliikumise analüüs Tobii Pro lahendustega

Ühe kaitsemeetme kohaselt on silmade liikumise ja fookuspunkti alusel võimalik kindlaks teha, kas kasutaja tegeleb parasjagu sisseastumistesti lahendamisega ja kas ta sooritab tegevusi ise (vt Lisa 2 jaotis 3). Selle kinnitamiseks läbi viidud uuringut sooritati Tallinna Tehnikaülikooli Innovatsiooni- ja ettevõtluskeskuses Mektory [53], kus on võimalik kasutada Tobii Pro silmajälgimislahendusi.

Kolme eriliigilise katse abil uuriti järgnevaid teese:

- Parasjagu külastatavat veebilehte on võimalik kindlaks määrata selle alusel, kuhu kasutaja veebilehel olles kõige sagedamini vaatab.
- Tegevuste, nagu pilgu ja hiire liikumine, järjestus sõltub sellest, kas RangeForce laborit sooritatakse ise või vaadatakse, kuidas lahendab ülesannet keegi teine.
- Pilgu liikumistrajektoor teksti lugemisel erineb trajektoorist, mis tekib meediasisu (fotod, videod) vaadates.

Alljärgnevalt on esitatud uurimuse jooksul kasutusel olnud riist- ja tarkvaralahendused, sooritatud katsed, tekkinud probleemid ja tulemused.

5.1 Töökoht

Antud uurimuses oli kasutusel infrapunase valgusega silmade liikumist jälgiv ja lindistav kaameraseade Tobii Pro X2-30 Eye Tracker (edaspidi ka Tobii Eye Tracker) [54]. Ühe sekundi jooksul 30 korda sensoritelt kasutaja silmade liikumise kohta infot küsiv seadis on kõigest 18.4 cm laiune ja sellest tulenevalt sobilik mitmeteks erinevateks uuringuteks alates reaalelulistest situatsioonidest telefoni- ja arvutiekraanidel toimuvani välja. Tobii Pro X2-30 sobib kasutajate silma fookuspunkti analüüsimiseks, kuid ei ole piisavalt väikese diskreetimistaktiga, et uurida täpsemat silma hüplemist ehk sakaade.

Jälgimisprotsessi ajal valgustab seadeldis kasutajat lähi-infrapunase (*NIR*) valgusega, mis peegeldub tagasi silma sarvkestalt [55]. Sensoritest saadud andmete alusel arvutatakse välja silmamunade asend ja pilgu täpne asukoht ekraanil ehk silmade fookuspunkt. Kuna silmade asukoha määramiseks kasutatakse infrapunast valgust, osutub takistuseks prilliklaasidelt peegelduv kuvarivalgus, mistõttu ei saa seda kasutada prillidega. Samuti raskendab jälgimisprotsessi liigne päevavalgus, mida oli Mektory laboris hoolimata ette tõmmatud ruloodest kellaajast sõltuvalt suuremal või vähemal määral.

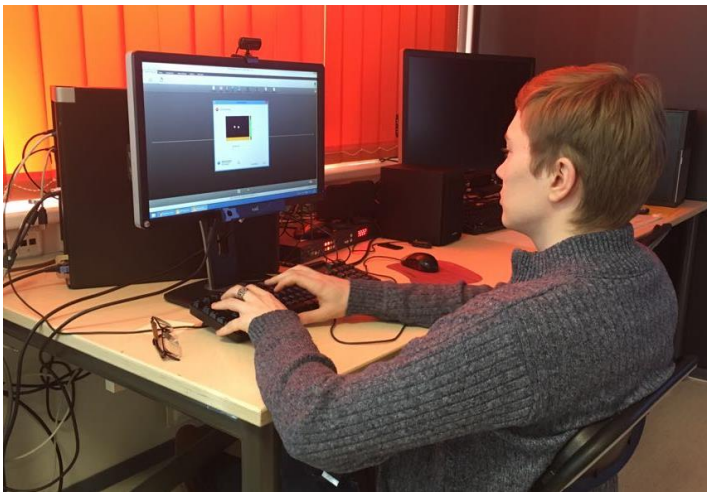
Tobii Eye Trackeri kasutaja ei ole kohustatud oma pead staatiliselt paigal hoidma, vaid võib seda mõningal määral liigutada ilma jälgimisprotsessi drastiliselt mõjutamata. Näiteks sensoritest 70 sentimeetri kaugusel istudes on lubatud pea liikumine 50 x 36 cm suuruses alas [56]. Samuti taastub süsteem koheselt kasutaja silmade pilgutamisest. Tobii Eye Trackeri töötamisvahemik on 40-90 cm kaugusel ekraanist.

Kleepribaga ekraani alaosa külge kinnitatud Tobii Eye Tracker oli USB-kaabli kaudu ühendatud Dell Precision T3600 tööjaamaga (vt Tabel 2). Kõikides katsetes kasutati sisendseadmetena Dell SK-3205 klaviatuuri ning esialgu Logitech'i arvutihiirt, kuid kuna uurimuse viimastel katsetel ilmnes Logitech'i hiirel kasutajate tegevust tugevasti häiriv defekt (katkine juhtmeühendus), oldi sunnitud see asendama hiirega firmalt HP.

Tabel 2. Eksperimendis kasutatud tööjaama tehnilised andmed.

Tööjaam	**Protsessor**	**Taktsagedus**	**Muutmälu (RAM)**	**Operatsioonisüsteem**
Dell Precision T3600	Intel® Xeon® CPU E5-1650	3.20GHz	16,0 GB	Windows 8 Pro, x64 (64-bitine)

Kasutaja näoilmet jälgiti kuvari ülaserva kinnitatud Acme CA04 välise veebikaameraga. Katsetes oli kasutusel 21.5-tolline Dell U2212HM LED-ekraan resolutsiooniga 1920x1080. Töökoht asus vahetult papiplaadi ja rulooga kinni kaetud akna all nii, et osalejad olid näoga akna poole suunatud (vt Joonis 12). Ruumi valgustasid luminofoorlambid ja läbi ruloo kumav päevavalgus.



Joonis 12. Töökoht (erakogu). Ekraani alaserva külge on kinnitatud kasutaja silmi jälgiv Tobii Pro X2-30 Eye Tracker ja ülaserva kasutajat ennast filmiv Acme CA04 kaamera.

Katsete koostamiseks, Tobii Eye Trackerist saadava info kogumiseks, visualiseerimiseks ja analüüsimiseks kasutati tarkvaralahendust Tobii Pro Studio versioon 3.2.3 (edaspidi Tobii Studio) [57]. Antud programm võimaldab stiimulina kasutada ülesannet kirjeldavaid juhendeid, küsimustikke, staatilisi pilte ja PDF-dokumente, dünaamilisi videoid, veebilehti ja kuvahõivet (*screen capture*) ning välisel seadmel (teler, teine arvuti) ja ruumis toimuvat (vt Joonis 13) [55].

Joonis 13. Tobii Pro Studio stiimulelementide valik testi seadistamise vaates.

Käesolevas uurimuses hõlmab testide koostamiseks kasutatud elementide kogu videoid, veebilehti ja kuvahõivet. Kuigi Tobii Studio võimaldab katset koheselt alustada eelnevalt kindlaks määratud veebilehelt, kasutades selleks testi koostamisel vastavat elementi (*web*), toetas Mektory arvutis olev versioon vaid Internet Explorer veebilehitsejat, kus RangeForce veebisait korrektselt ei avanenud, mistõttu otsustati veebielemendi asemel kuvahõive kasuks ning uurimuse all olevad veebilehed avati taustal manuaalselt enne katse algust.

5.2 Katsete ülesehitus

Uurimus koosnes kolme liiki alamkatsetest (vt Tabel 3), mille raames üritati leida erinevusi kasutajate käitumises sisseastumistesti iseseisvalt sooritades, kellegi teise sooritust jälgides ja vähemalt ühel meediasisuga veebilehel (Postimees, YouTube)

tavapäraseid toiminguid tehes. Postimehe [58] ja YouTube'i [59] veebilehed valiti kui ühed sageli kasutatavad veebisaidid. Kuna Tobii Studio salvestab kuvahõive, klaviatuuri ja hiire sisendi, otsustati osalejate privaatsuse käesolevast uurimusest välja jätta sotsiaalmeedia veebileheküljed, nagu Facebook või Instagram. Katseülesannete täitmise ajal salvestati osalejate nõusolekul nende näoilmeid, silmade liikumist, sisendseadmete kasutust ja ruumiheli.

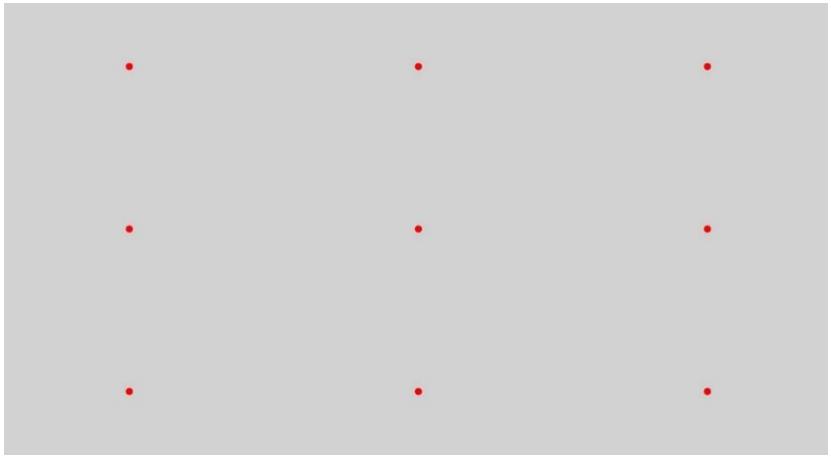
Tabel 3. Katsed.

Katse tüüp	**Katses kasutatav materjal**	**Katse jooksul salvestatav materjal**	**Kirjeldus**	**Eesmärk**
Vaatamine	Eelnevalt lindistatud ekraanivideo RangeForce keskkonnas labori lahendamisest	Kasutajavideo, ruumiheli, silmade liikumine	Osaleja jälgib ligikaudu 10 minutit kestvat ekraanivideot sellest, kuidas keegi teine lahendab RangeForce keskkonnas laborit. Keelatud on sisendseadmete (klaviatuur, hiir) kasutamine. Katse lõppeb ekraanivideo lõppedes.	Simuleerida olukorda, kus kaitsemeetmeks on näotuvastus ja silma fookuspunkti analüüs. Võrrelda kasutaja silmade liikumist laborit ise sooritades ja kellegi teise sooritust jälgides.
Sooritus	RangeForce labor	Ekraanivideo, kasutajavideo, ruumiheli, silmade liikumine, hiirevajutuse asukoht, klahvivajutuse ajahetk ja identifikaator	Osaleja sooritab iseseisvalt RangeForce keskkonnas sissejuhatavat laborit (Apache veebiserveri konfigureerimine). Lubatud on kasutada internetti abi otsimiseks, kuigi labori keskkonnas antavad juhised on piisavalt põhjalikud, et nende baasil labor sooritada.	Simuleerida situatsiooni, kus kasutaja ei riku eksamikorda, sooritab labori üksinda ruumis viibides iseseisvalt ja ilma keelatud abimaterjale lahendamata. Võrrelda kasutaja silmade liikumist laborit ise sooritades ja kellegi teise sooritust jälgides.

Katse tüüp	Katses kasutatav materjal	Katse jooksul salvestatav materjal	Kirjeldus	Eesmärk
Muu	Postimehe veebileht, YouTube veebileht	Ekraanivideo, kasutajavideo, ruumiheli, silmade liikumine	Kasutajal on lubatud veebilehel ilma piiranguteta ringi liikuda, alamlehti avada, artikleid ja videoid vaadata.	Võrrelda kasutaja silmade liikumist RangeForce keskkonnas ja muudel veebilehtedel.

Katsete summaarne kestus oli ligikaudu üks astronoomiline tund, varieerudes muu valdkonna veebilehel (Postimees, YouTube) viibitud ajast ning labori sooritamise kiirusest tulenevalt. Kuna Mektory labori näol on tegemist maja päikesepoolses küljes asuva ühiskasutuses arvutiklassiga, ei olnud võimalik kõiki kaitseid sooritada samades tingimustes. Katseid sooritati mitmel eri päeval ajavahemikus alates kella üheksast hommikul kuni kella üheksani õhtul, mis tähendab, et kuigi ruumis põlesid alati luminofoorlambid ja aknad olid ruloodega blokeeritud, varieerusid valgustingimused päevavalgusest tulenevalt.

Enne iga katset teostati täpsuse suurendamiseks korduvkalibreerimine, kasutades üheksat punkti ekraanil. Kalibreerimise ajal ilmus ekraanile musta sisuga punane ring, mida kasutaja pidi pilguga jälgima, kui see läbis ekraanil ringi liikudes kõik üheksa kalibreerimispunkti (vt Joonis 14).



Joonis 14. Kalibreerimispunktide asukohad ekraanil.

Kui kalibreerimine oli piisavalt täpne, paluti osalejatel oodata, kuni test käivitub, vastasel juhul läbiti kalibreerimisprotsess uuesti. Video vaatamise test lõppes ilma kasutajapoolse

sekkumiseta, kuid kuvahõive testide puhul lõpetas osaleja testi ise eelnevalt saadud juhistele toetudes.

Osalejad viibisid katsete sooritamise ajal ruumis üldiselt üksinda, imiteerimaks ideaalset kodust eksamikeskkonda. Erandiks oli vaid kaks vaatluskatset, kus ruumis viibis lisaks katses osalejale katset läbi viiv isik, kuid kummalgi juhul ei toimunud isikute vahel suhtlust ning katsete tulemused ei kajasta märkimisväärset erinevust üksinda ja mitmekesi ruumis viibitud katsete vahel. Võimalik, et tulemusi oleks mõjutanud see, kui mitmekesi ruumis viibides oleks isikutel lubatud omavahel rääkida või muul moel infot edastada, kuid antud töö skoopi arvesse võttes tuleb seda aspekti hiljem edasi uurida.

5.3 Osalejad

Uurimuses osalejate valim hõlmas esialgu üheksat Tallinna Tehnikaülikooli infotehnoloogia teaduskonna tudengit vanusevahemikus 21-31 eluaastat, kuid kuna kolmel neist oli raskusi ilma prillideta arvutiekraanil oleva teksti 50 sentimeetri kauguselt nägemisega, taandus uurimuses osalev grupp kuuele inimesele (vt Tabel 4), kellest üks oli sunnitud RangeForce labori lahendamiseks ekraanil olevat teksti suurendama ning üks loobus vähese kokkupuute tõttu Linuxi käsureaga laboriülesande iseseisvast lahendamisest. Kokku osales uurimuses niisiis neli meest ja kaks naist, kõik neist europiidse rassi esindajad ja mitte ükski varasemalt RangeForce keskkonnaga kokku puutunud.

Tabel 4. Uurimuses osalejate info. Sugu: N - naine, M - mees. Katsete teostamise järjekord: X - muu, S - sooritus, V - vaatamine.

Osaleja kood	**Sugu**	**Silmavärv**	**Nägemine**	**Osalus uurimuses**	**Katsete teostamise järjekord**
O1	N	roheline	prillid	täielik	XSV
O2	M	roheline	korrigeerimata	täielik	XVS
O3	M	sinakashall	korrigeerimata	täielik	SXV
O4	M	hall	prillid	täielik	VSX
O5	M	roheline	prillid	mööndustega	VXS
O6	N	sinakashall	korrigeerimata	osaline	XV

Osalejad läbisid katsed erinevas kombinatoorses järjekorras (vt Tabel 4). Kaks osalejat sooritasid esmalt labori iseseisvalt ja vaatasid seejärel kellegi teise sooritust, kolm osalejat jälgisid eelnevalt labori kuvahõivet ja said seejärel ülesandeks sama labor ise läbida ning üks osaleja loobus labori tegemisest. Muu kategooria ülesanne teostati kas enne või pärast RangeForce'i omi või nende vahepeal. Järjekorra varieerumise põhjuseks oli uurida, kas tulemused sõltuvad sellest, kas osaleja on ülesandega eelnevalt kokku puutunud.

5.4 Probleemid

Uurimuse teostamise faasis ilmnes nii mõnigi takistav faktor. Näiteks ei oldud esialgu arvestatud sellega, et kõigi uuringus osalejate nägemine ei võimalda neil ilma korrigeerivate vahenditeta Tobii Eye Trackeri kasutamiseks vajalikult kauguselt ekraanil olevat teksti näha. Prille ei saanud kanda, kuna need takistasid infrapunase valguse abil pupillide asukoha määramist. Kuigi lõplikus valimis esines ka isikuid, kes olid vajadusel valmis katse sooritamiseks läätsi kasutama, ei olnud see tarvilik, kuna nad nägid ekraanil olevat teksti piisavalt selgelt ka ilma nendeta. Üks uuringus osaleja oli sellegipoolest sunnitud RangeForce labori sooritamiseks kuvapilti suurendama ning isegi pärast seda liikus ta peaga Tobii Eye Tracker'i sensoritele ohtlikult lähedale, väljudes äärepealt jälgimisvahemikust.

Osalejad tõid esile, et võõra riistvaraga oli ülesande lahendamine ebamugavam, kui see oleks olnud harjumuspärast arvutit kasutades. Üks osaleja oli igapäevaselt harjunud kasutama ingliskeelset klaviatuuri ning oli seetõttu sunnitud poole soorituse pealt klaviatuuri keelt vahetama, häirides tema loomulikku töö kulgu. Poole uuringu peal ilmnes algselt kasutatud arvutihiire juhtmel defekt, mistõttu ühendus hiire ja arvuti vahel katkes sageli ning häiris uuringus osalejate toiminguid. Seetõttu otsustati edasistes katsetes vigane hiir asendada.

Lisaks kurtis üks katsetes osaleja ka toolide ebamugavust. Kuigi osalejatel oli lubatud testide vahel vabalt ringi liikuda ja sirutada, loobusid paljud sellest võimalusest. Kahjuks ei olnud võimalik ka töökohal olevat tooli vahetada, kuna laboris olidki ainult üht tüüpi plastmasstoolid.

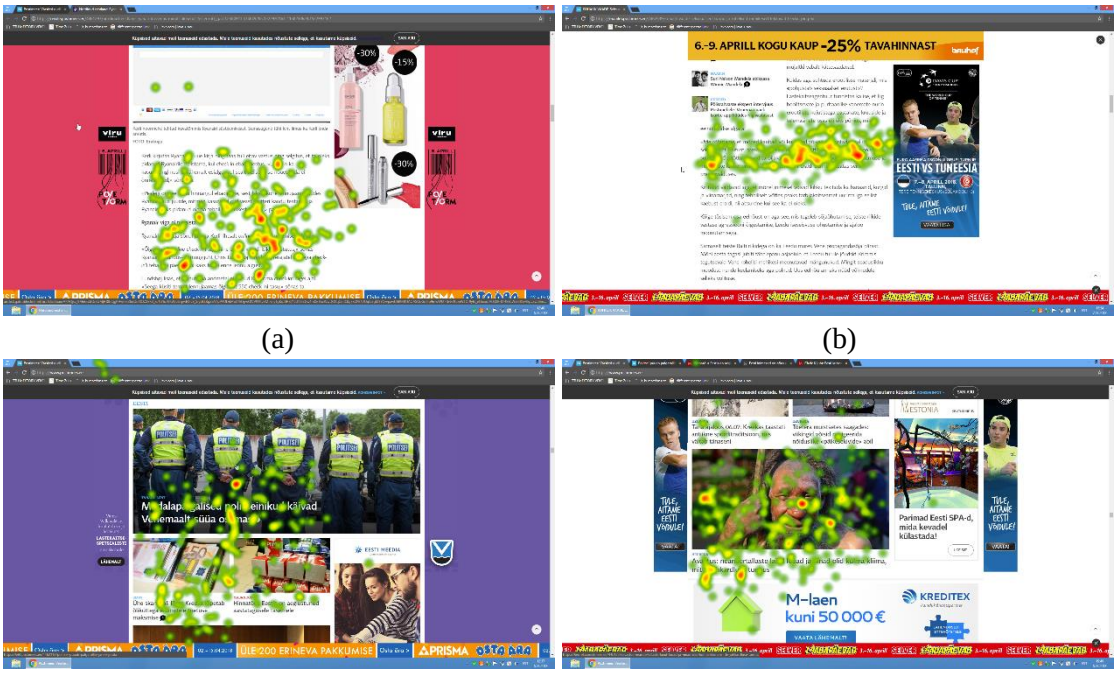
5.5 Tulemused

Kuna katses osalejaid oli lõplikult kokku kuus, on valim liiga väike, et selle alusel laiemaid üldistusi teha, ning põhjalikumaks otsustamiseks tuleks katset korrata enamate inimestega. Küll aga on võimalik ka kuueliikmelise grupi pealt juba mõningaid järeldusi teha. Alljärgnevalt ongi välja toodud katsete tulemused ja nende põhjal tehtud soovitused.

5.5.1 Soojuskaardid

Veebilehe ülesehitusest tulenevalt võib eeldada, et mõni osa leheküljest saab kasutajalt rohkem tähelepanu kui teine. See oletus saab kinnituse, kui vaadata Postimehe ja YouTube veebilehe ning RangeForce labori soojuskaarte (*heatmap*) (vt Joonis 15, Joonis 16, Joonis 17), mis annavad visualiseeritud ülevaate sellest, kui sageli kasutaja pilk teatud piirkonnas peatus [55]. Kuumkohad ehk arvuliselt kõige sagedamini tähelepanu pälvinud alad on antud töö soojuskaartidel märgitud punasena ning harvem vaadatud piirkonnad rohelisena. Soojuskaartide visualiseerimise aluseks olev ajavahemik varieerus poolest minutist viie minutini, sõltuvalt veebilehe sisu dünaamilisusest, vaataja käitumisest ning kerimistempost. Kiirelt muutuva sisu puhul (Postimees, YouTube) koostati soojuskaart lühema ajavahemiku kohta kui RangeForce labori korral, kus sisu paigutus muutus vähe.

Postimehe veebivaates on sisu vertikaalselt joondatud lehe keskossa ning ääred on tühjad või sisaldavad reklaami (vt Joonis 15). Sellest tulenevalt on ka kasutaja pilk suunatud enamasti lehe keskossa, moodustades seal ühtlase pilgupunktide klastri. Ühtegi ülejäänutest intensiivselt eristuvat kuumkohta Postimehe soojuskaartidel ei esine.



(a) (b)

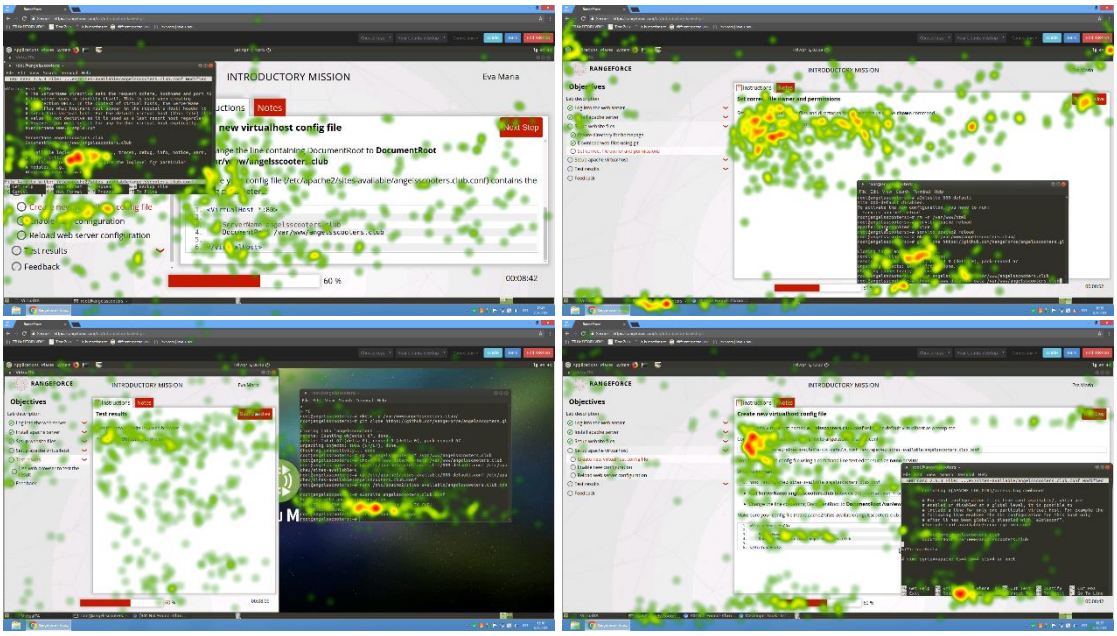
(c) (d)

Joonis 15. Postimehe veebilehe soojuskaardid: (a), (b) artikli lugemine; (c), (d) pealehe sirvimine.

YouTube'i veebilehe puhul sõltub soojuskaart suuresti sellest, kas videoid vaadati täisekraanvaates või minimeeritult (vt Joonis 16). Viimast on võimalik soojuskaardi põhjal kindlaks määrata, kui pilk on koondunud pigem ühte piirkonda. Täisekraanvaate puhul ühtlast joont ei eristu - soojuskaart sõltub vaadatud videost ja selles olnud pilkupüüdvatest objektidest.

Joonis 16. YouTube'i soojuskaardid.

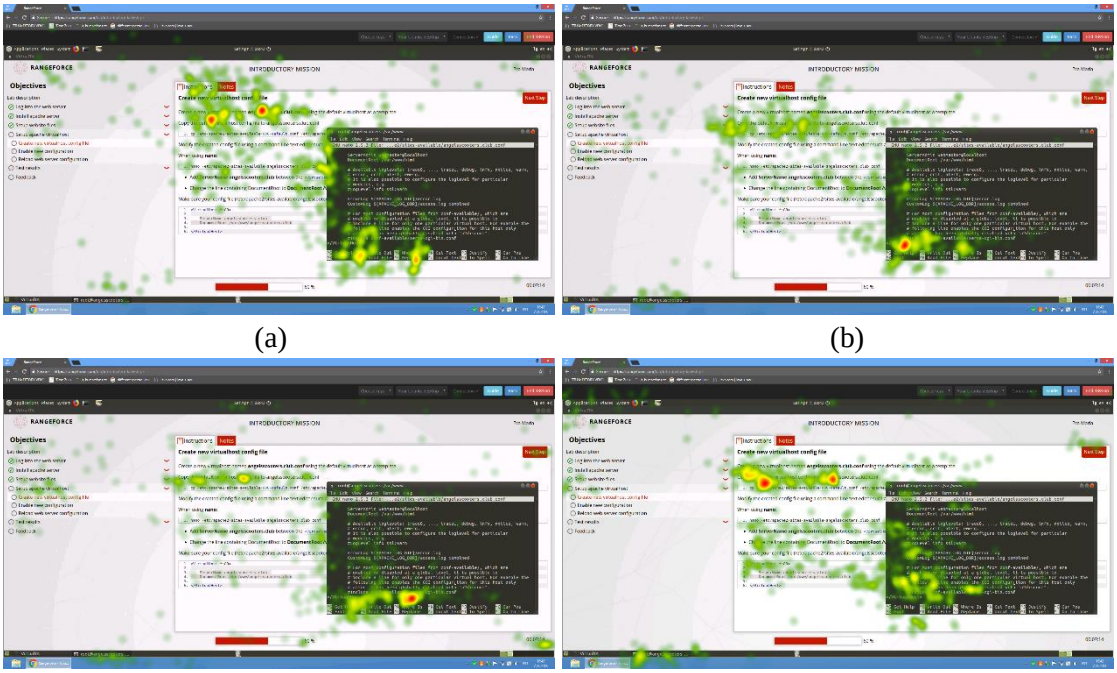
RangeForce labori veebileht hõivab kogu veebilehitseja akna, ulatudes nii horisontaalselt kui vertikaalselt servast servani. Labori soojuskaardid erinevad suuresti katses osalejate lõikes (vt Joonis 17). Eristuvad mõningad kuumkohad, nagu järgmise sammuni viiv nupp virtuaalmasina ülemises paremas servas, terminalisakk tegumiribal, tekstijuhiseid sisaldav ala, labori etappe näitav loetelu ja terminaliaken, kuid need sõltuvad sellest, kuidas on kasutaja paigutanud rakenduste aknad. Kuigi akende paigutusele piiranguid seatud polnud ning neid võis korduvalt ümber tõsta, oli enamikul katses osalejatest ülesande edenemist ja juhiseid sisaldav aken täisvaates, välja arvatud üks osaleja, kes muutis poole katse pealt juhisakna asukohta. Terminaliaknaid seevastu liigutati sageli, kuna täisekraanil juhiseid kuvades kippus too ülesande kirjeldust osaliselt katma.



Joonis 17. RangeForce labori akende erinevad paigutused ja vastavad soojuskaardid.

Eelnevast võib järeldada, et kasutaja pilgu soojuskaart ei ole piisav, et selle alusel üheselt määrata, millist keskkonda parasjagu kasutatakse. Kuigi võimalik on eristada veebilehti, mille sisu on koondunud ekraani keskele, nendest, mis katavad ekraani kogu ulatuses, sõltub RangeForce keskkonna soojuskaart sellest, kuidas liigutab kandidaat virtuaalmasina programmiaknaid. Seda, kas kaamera ees viibiv isik jälgib parasjagu RangeForce keskkonda, saab kontrollida labori staatiliste objektide, nagu nupud, menüüd, tegumiriba sakid, baasil. Kui kasutaja pilk peatub mainitud elementidel harva või üldse mitte, on alust arvata, et ekraanil kuvatakse parasjagu mõnd muud keskkonda ja toimumas on kehastusrünnak, kus näotuvastust teostav kaamera on suunatud ühe isiku poole, aga ülesannet lahendab vaateväljast eemal asuv abiline.

Olukorras, kus ekraanid on dubleeritud, ehk tegelik kandidaat jälgib variisiku tegevusi lisaekraani vahendusel, ei ole soojuskaardid eristatavad (vt Joonis 18). Kuna lehel kuvatavad elemendid on samad, on varieeruvus nende vaatamise sageduse vahel minimaalne, mis tähendab, et selle alusel ei ole võimalik eristada, kas kaamera ees olev isik tegeleb testi lahendamisega ise või jälgib, kuidas seda teeb keegi teine.



(a) (b)

(c) (d)

Joonis 18. Vaatlejate ja sooritaja viie minuti fookuspunktide baasil koostatud soojuskaartide võrdlus: (a), (b), (c) vaatlejate soojuskaardid; (d) sooritaja soojuskaart.

Tulemustest võib järeldada, et RangeForce süsteemis lahendatava sisseastumistesti puhul on pilgu fookuspunktidel pigem toetav roll veebikeskkonna kindlaks määramisel ning ainult kuumkohtade alusel ei ole võimalik teha otsuseid isiku kohta, kelle poole on suunatud silmade liikumist jälgiv kaamera.

5.5.2 Pilgu ja kursori korrelatsioon

Teisena uuriti hüpoteesi, mille kohaselt kasutaja silmade liikumine ja hiire kasutamine, spetsiifilisemalt antud tegevuste järjekord, on sõltuvuses sellest, kas kasutaja sooritab toiminguid ise (edaspidi sooritaja) või jälgib näiteks lisaekraani vahendusel, kuidas seda teeb keegi teine (edaspidi vaatleja). Eelduse kohaselt on esimesel juhul tegevuste järjekord järgmine:

1. Sooritaja suunab pilgu elemendile või selle vahetusse lähedusse.

2. Sooritaja liigub kursoriga elemendile.

3. Toimub interaktsioon (näiteks hiireklikk) kasutaja ja elemendi vahel.

Selle kinnitamiseks paluti uuringus osalejatel labor lahendada iseseisvalt, üksinda ruumis viibides ilma kelleltki teiselt juhiseid saamata.

Kommunikatsiooni puudumisel ehk kui sooritaja ei edasta vaatlejale juhiseid oma tegevuste kohta, võiks olukord olla selline:

1. Kursor liigub elemendile.

2. Vaatleja jälgib pilguga liikuvat kursorit või kohta, kus kursor liikumise lõpetas.

3. Toimub interaktsioon kasutaja ja elemendi vahel.

Laboris oli saadaval üks pilgujälgimisseade, mis võimaldas samal ajal jälgida ainult üht osalejat. Seetõttu ei olnud võimalik tekitada olukorda, kus laborit lahendab variisik ning pilgupunkti jälgija petmiseks kasutatakse kaht ekraani, millel on dubleeritud pilt RangeForce labori keskkonnast. Sellest tulenevalt lindistati Tobii Studio abil esmalt kuvahõive kahe osaleja sooritusest, mida näidati hiljem osalejatele video kujul. Taolise simulatsiooni abil oli võimalik kõrvutada sooritaja ja jälgijate silmade liikumist.

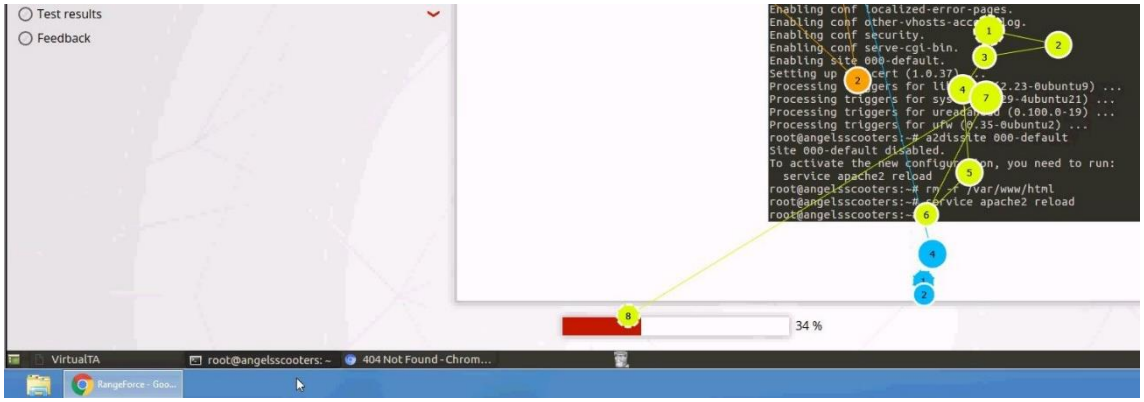
Uurimisküsimus saab kinnitust juba ainuüksi visuaalse vaatluse käigus (vt Joonis 19), kus on näha, et lõpetades tegevuse terminaliaknas, suunab labori sooritaja pilgu tegumiribal olevale veebilehitseja avamise sakile sooviga terminalis tehtud käskude tulemust kontrollida. Kui kasutaja on pilguga paika pannud saki asukoha, liigutab ta selle lähedusse hiirekursori, valmistudes pärast kursori asukoha korrigeerimist sakile vajutama. Katses kogutud arvandmete kohaselt keskendub sooritaja antud joonisel kujutatud klikitava punkti lähipiirkonda ($\pm$67 pikslit) ligikaudu pool sekundit enne vajutuse toimumist.

Vaatlejad seevastu ei tea, mis tegevust sooritaja järgnevalt teha tahab ning jälgivad pilguga terminaliakent, kus toimus viimane tegevus, kuni märkavad kursori liikumisest, et fookuspunkt on muutunud. Kuna tegumiribal veebilehitseja ikooni klikkimine avab uue akna, haarab vaatlejate tähelepanu hoopis avanenud rakendus ning kuigi nende pilgud liikusid esialgu tegumiriba suunas, ei jõudnud antud juhul ühegi vaatleja pilk vajutatud nupuni, vaid liikus avanenud aknasse.

Samuti ei pööranud sooritajad hiire liigutamise kiirusele teadlikult tähelepanu, millest tulenevalt muutus kursori asukoht ekraanil kohati kiirelt ja hüplikult, tehes vaatlejatele kursori jälgimise keerulisemaks. Sellisel juhul keskendusid vaatlejad tempokama liikumise korral kursorile alles siis, kui see oli peatunud.

(a)

(b)



(c)

Joonis 19. Korrelatsioon pilgu ja hiire liikumise vahel: (a) ajahetkel t-1 suunab labori sooritaja pilgu tegumiriba brauserisaki poole, kursor asub terminaliaknas; (b) ajahetkel t liigutab labori sooritaja kursorit saki suunas, kursor asub tegumiribal; (c) ajahetkel t liigub üks sooritaja vaatajatest pilguga tegumiribal asuva kursori suunas, ülejäänud vaatavad alles terminaliakent.

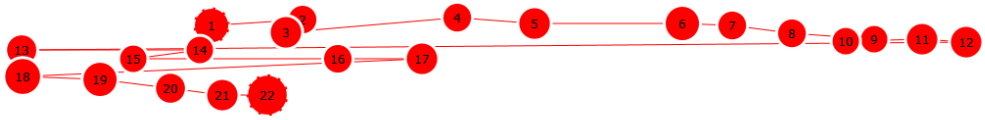
Juhuslike hiirevajutuste puhul, näiteks kogemata hiireklahvile vajutades või soovides taustal olevat akent aktiveerida, ei esine äratuntavat seost vajutuse asukoha, pilgupunkti ja tegevuste järjekorra vahel.

Kuna neli osalejat ei teadnud ja kaks osalejat teadsid enne katses osalemist uurimuse tagamaid, on võimalik võrrelda, kuidas erineb käitumine jälgimise ja sooritamise puhul olukorras, kus süsteemi ei üritata petta või petetakse tahtlikult. Need, kes olid katse ülesehitusest ja eesmärgist teadlikud (edaspidi ennustajad), said ülesandeks sooritaja tegevusi ette ennustada ja vastavalt sellele oma pilku enne hiire liikumist suunata.

Kuigi ennustajad reageerisid hiire liikumisele aktiivsemalt, ei olnud kumbki neist võimeline pilguga järgmisena fookusesse sattuvat elementi jälgima enne, kui sooritaja oli elemendile keskendunud ja paljastas kursori liikumise sihi. Kui liikumissuund oli juba teada, suutsid mõlemad ennustajad ekraanil olevate elementide seast kindlaks määrata selle, milleni sooritaja liigub. Ennustada oli keerulisem, kui sooritaja tegevus kaldus kõrvale tavapärasest labori kulust, näiteks avati kogemata vale aken. Lähemat uurimist vajab situatsioon, kus sooritaja ja vaatleja saavad omavahel suhelda, et tegevuste kohta infot vahetada.

5.5.3 Keskkonna ja silmade liikumise seos

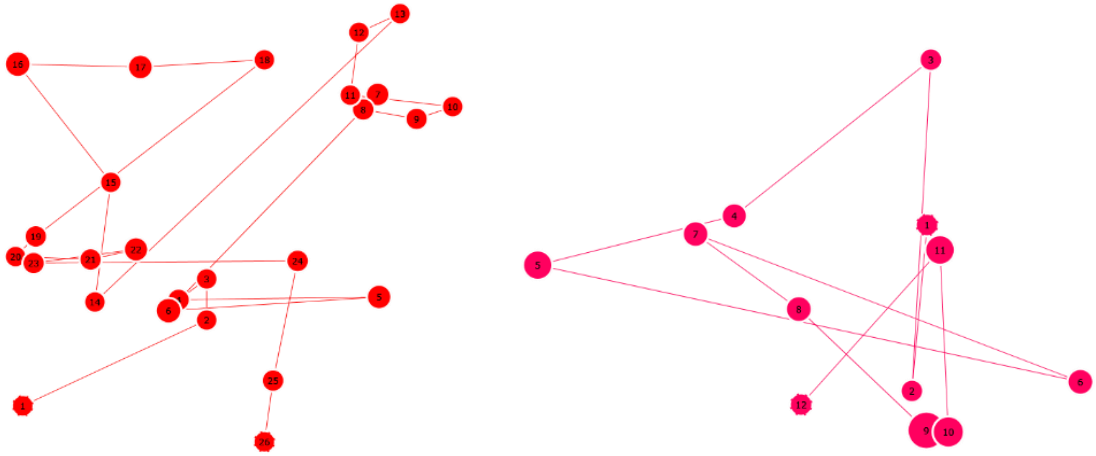
Seda, millega kasutaja parasjagu tegeleb, on võimalik osaliselt kindlaks määrata pilgu liikumise järgi arvutiekraanil. Näiteks tekstilist sisu lugedes liigub pilk üldjuhul ridade kaupa vasakule paremale ja ülalt alla (vt Joonis 20).



Joonis 20. Silmade liikumine teksti lugedes.

Suuremal hulgal graafilist sisu (pildid ja videod) sisaldavas keskkonnas liigub pilk hüplikumalt (vt Joonis 21). Postimehe pealehel liiguvad silmad paremalt vasakule uudiste pealkirjade lugemise ajal, kajastudes joonisel horisontaalsete joontena, kuid reklaamid ja uudiste pealkirjade kohal juures olevad fotod hajutavad pilku ka diagonaal- ja

vertikaalsihis. YouTube'i keskkonnas täisekraanil videot vaadates on pilk veelgi enam hajutatud, peatudes vaid tol ajahetkel videos olevatel pilkupüüdvatel objektidel.



(a) (b)

Joonis 21. Silmade liikumine graafilisemas keskkonnas: (a) Postimeest lugedes, (b) YouTube'i videot vaadates.

Eelnevast tulenevalt saab pilgu trajektoori jälgimist kasutada keskkondades, kus on rohkem tekstisisu. Kuna RangeForce laborite puhul kuvatakse enne labori algust taustaloo ja ülesande kirjeldus ning tekstilisi juhiseid on antud ka labori sooritamise ajal, oleks võimalik jälgida, kas kasutaja pilk liigub paremalt vasakule, kui parasjagu on aktiivne tekstilist sisu sisaldav aken. Kui trajektoor on ebaühtlane ja hüplik, liikumata kordagi horisontaalsihis, on alust arvata, et kaamera ees viibiv isik ei tegele teksti lugemisega. See võib tähendada, et ta jälgib kellegi teise sooritust ilma ülesande juhistesse süvenemata või kasutab hoopis mõnd muud graafilise sisuga keskkonda.

5.5.4 Sisendseadmete kasutus

Kõik ülesande lahendamiseks vaja minevad käsud olid ette antud juhisaknas. Ilmnes, et uuringus osalejad kasutasid käskude sisestamiseks nelja eri meetodit ja nende kombinatsioone:

- Käskude kopeerimine ja kleepimine hiirega.
- Käskude kopeerimine ja kleepimine kiirklahvide ehk klaviatuuriklahvide kombinatsiooniga.

- Käskude sõna-sõnaline ümber trükkimine konsooli.
- Käskude osaline trükkimine konsooli koos nende automaatse lõpetamisega tabulaatorklahvi (*tab*) abil.

See annab laialdast infot kasutaja eelistuste kohta ning võimaldab osalejatel vahet teha ainuüksi valitud käsusisestusmeetodi põhjal. Kui soovida suurendada analüüsiks kogutud andmestikku, võib trükkimisdünaamika järgi kasutaja tuvastamiseks keelata hiire ja klaviatuuri kopeerimise ja kleepimise funktsioonid. See sunnib kõiki sooritajaid käske manuaalselt terminaliaknasse ümber kirjutama. Tabulaatorklahvi keelamise vajadust ei peeta oluliseks, kuna selle kasutamine või mittekasutamine on kasutajaspetsiifiline, mistõttu antud aspekt võib olla üheks faktoriks, mille alusel kasutajate trükkimisstiile eristada.

Kuigi kõik osalejad olid pädevad arvutikasutajad, vaadati soorituse ajal trükkimist alustades mõnikord siiski klaviatuuri suunas. Vaatlejad, kellel polnud võimalik klaviatuuri ega hiirt kasutada, videos toimuva trükkimisprotsessi ajal laua suunas ei vaadanud. Klaviatuuri suunas unustasid sageli vaadata ka ennustajad, kelle ülesandeks oli ettekujuteldavat kaitsesüsteemi petta, kuid see võis tuleneda ka sellest, et nad ei omanud põhjalikku ülevaadet potentsiaalsetest kaitsemeetmetest.

Kuna tegemist oli osalejate jaoks võõra ja harjumatu arvutiga, ei saa üheselt väita, et klaviatuuri vaatamine trükkimise algul toimub igakordselt. Kinnitamaks, et kõik sooritajad vaatavad ka oma personaalarvutis trükkides alati vähemalt korra sisendseadme poole, tuleb teostada lisauuring. Samas võib antud uurimuse tulemustele toetudes pidevat sisendseadme pilguga eiramist kasutada eksamikorra rikkumise riski tõenäosuse suurendamiseks.

5.5.5 Muud tähelepanekud

Võiks eeldada, et neil osalejatel, kes läbisid enne vaatluskatse ja seejärel labori soorituse, kulus labori lahendamisele vähem aega, kuid antud uurimuses osalejate puhul see alati nii ei olnud. Sageli kiirustati laborit lahendades, mistõttu jäid mõned asjad kahe silma vahele ning ühel osalejal kulus vigade korrigeerimise tõttu labori sooritamisele lausa kahekordne aeg kui teistel.

Esines mõningaid erinevusi labori vaatlejate ja sooritajate käitumises. Kui sooritajad olid enamasti aktiivselt ülesandele pühendunud ja vaatasid harva ekraanilt kõrvale, siis vaatlejad tegid seda sagedamini ning eriti siis, kui vaatluskatse oli pärast soorituskatset. Vaatlejad olid tihti toolis tahapoole nõjatunud, kuna neil puudus vajadus kasutada sisendseadmeid. Sooritajad seevastu istusid kaamerale lähemal ja olid püstisemas asendis.

Kui soorituskatse ajal olid osalejad enamasti keskendunud, siis kellegi teise lahendust vaadates ja Postimehe ning YouTube'i veebilehtedel ringi navigeerides varieerus osalejate miimika suuresti (vt Joonis 22). Emotsioonid võisid olla üle pingutatud, kuna uuringus osalejad teadsid, et nende tegevusi salvestatakse. Sooritustkatse ajal olid osalejad pigem keskendunud ning mõnikord isegi frustratsiooni väljendava pilguga. Seetõttu sai kinnitust oletus, et miimika võib olla üheks kaitsemeetmeks, et vältida kehastusrünnet ja tuvastada olukorda, kus kaamera ees viibiv isik tegeleb kõrvaliste asjadega. Samas ei ole võimalik üheselt välistada, et kandidaadi miimika ei või RangeForce sisseastumistesti ajal laialdaselt varieeruda, mistõttu ei saa ainuüksi näoilme muutumisest eksamikorra rikkumist järeldada.

Joonis 22. Erinevad reaktsioonid vaatamise ja muud tüüpi katsetel (erakogu).

Üks osaleja rääkis ülesannete ajal valjuhäälselt iseendaga, kusjuures tegemist olevat tema tavapärase kombega. Ülejäänud osalejad olid katsete sooritamise ajal üldjuhul vait, aeg-ajalt esines vaid köhatamist, haigutusi või nihelemisega kaasnevaid helisid. Sellest tulenevalt saab kinnitust fakt, et kui kaitsemeetmena on kasutusel ruumihelist inimkõne tuvastamine, tuleb kandidaatidele selgitada, et testi sooritamise ajal peab ruumis valitsema vaikus.

Kuigi katses osalejatele ei olnud eelnevalt võimalikke ründeid tutvustatud, toodi pärast katseid uurimuse tausta selgitamise peale esile ründevõimalus, kus vahetult arvutiekraani alla on asetatud lisaseade, nagu mobiiltelefon, tahvel- või sülearvuti, mida kasutatakse sisseastumistesti ajal kõrvalise abi saamiseks. Lisaseadme poole vaatamist on kerge segi ajada klaviatuuri vaatamisega, mistõttu saab püstitada kaks väidet:

- kui kandidaadi pilk on suunatud alla, kuid sisseastumistestiks kasutataval arvutil puudub klaviatuurisisend, on võimalus, et infovahetuseks kasutatakse vahetult ekraani all asuvat lisaseadet;

- kui ruumihelis on kosta klahvivajutusi, kuid arvutil puudub klaviatuurisisend, kasutatakse suure tõenäosusega klaviatuuriga lisaseadet.

Antud tähelepanekud vajavad edasist uurimist, tegemaks kindlaks nende kasutamise võimalikkuse eksamikorra rikkumise tuvastamiseks.

6 Olemasolevate JavaScripti võimaluste katsetamine

Internetis on saadaval palju tasuta teeke ja lahendusi, mida võiks kasutada varasemalt mainitud kaitsemeetmete teostamiseks. Käesolevas peatükis on lähemalt uuritud mõnd JavaScripti lahendust, mis võimaldavad tuvastada inimkõnet, nägusid ja silmade liikumist, kui potentsiaalseid abivahendeid veebipõhiste eksamite järelevalve teostamiseks.

Nende hõlpsamaks testimiseks on koostatud algeline veebirakendus[1], kasutades HTMLi, CSSi, JavaScripti, BootStrapi[2] ja jQuery't[3]. Veebirakenduse kasutajaliides koosneb välistelt rakendusliidestelt saadud infot sisaldavast tabelist, nuppudest, millega käivitada isikutuvastuse funktsioone, pilgujälgimise kalibreerimisväljast ja veebikaamera videovoogu kuvavast elemendist. Kuna tegemist on veebilehitsejas avatava saidiga, mis ei takista kasutaja arvutis teiste programmide avamist, ei ole antud rakendus sobilik järelevalve teostamiseks, küll aga võimaldab katsetada olemasolevaid lahendusi.

Kõik alljärgnevad uuringud on teostatud 64-bitise Windows 10 operatsioonisüsteemi kasutava Lenovo W540 mobiilse tööjaamaga, millel on 2.80GHz Intel® Core™ i7-4810MQ protsessor, 8.00 GB muutmälu, 15.6" peegeldumisvastane ekraan resolutsiooniga 1920 x 1080, integreeritud 720p HD kaamera ja mikrofon. Kuna sisendseadmed, sealhulgas veebikaamera ja mikrofon, on arvutile sisse ehitatud, ei ole väliseid lisaseadmeid kasutatud.

6.1 Ruumiheli analüüs ja kõnetuvastus Web Speech rakendusliidesega

W3C ehk rahvusvahelise Interneti ja veebiga tegelevate firmade konsortsiumi Web Speech API ehk rakendusliidese eesmärgiks on hõlbustada arendajatel veebibrauseris kasutada kõnetuvastust, näiteks inimkõne muutmiseks tekstisisendiks, veebilehel kuvatud

[1] https://github.com/3v4m4r14/invigilation-tests-bsc

[2] https://getbootstrap.com/

[3] https://jquery.com/

teksti esitamiseks inimkõnena, häälkäskude rakendamiseks või otsingu teostamiseks [60]. Veebirakenduse leheküljele navigeerides küsitakse kasutajalt luba mikrofoni kasutamiseks, mida on vaja võimaldada kõnetuvastuse töötamiseks. Kõnet saab tuvastada ühekordselt või pidevalt. Käesoleva töö raames on ruumihelist inimkõne pidevaks tuvastamiseks kasutatud Web Speech API SpeechRecognition liidest. Kahjuks töötab antud liides töölauabrauseritest vaid Google Chrome'is [61], mistõttu kehtib edasine tekst vaid tolle veebilehitseja kohta.

Programmeeritud lahendus on äärmiselt elementaarne, kuna eesmärgiks on vaid inimkõne esinemise tuvastamine ruumi helipildis (vt Lisa 3). Samuti ei ole oluline, mis keeles kasutaja räägib. Sellest tulenevalt on määramata jäetud keele atribuut, mis tähendab, et keel määratakse HTML-dokumendi või kasutajaagendi keelesätete järgi ja on vaikimisi ingliskeelne [61]. Pideva tuvastamise tagamiseks on *continuous*-atribuut seatud tõeseks. Kui tuvastatakse kõnelemise algus või lõpp, kuvatakse vastav info veebirakenduse ülevaatlikus tabelis ning konsooli logitakse vastav märge koos ajatempliga. Lõpliku lahenduse korral salvestataks tegevuslogi konsooli asemel spetsiaalsesse logifaili, kuid liideste testimisel piisab ka info väljastamisest konsooli. Kõne lõppedes tehakse ühtlasi kõnetuvastusele taaskäivitus. Chrome'i veebilehitseja lõpetab teatud aja möödudes kõnetuvastuse [62], mistõttu tuleb see manuaalselt uuesti käivitada. Kui programmikoodis taaskäivitust ei tehta, lõppeb ruumihelist inimkõne tuvastamine.

Katsetest ilmneb, et autori koostatud lahendus suudab vaikses ruumis edukalt tuvastada kõnelemise algust. Kõnelemise lõpu kohta saabub info mõninga viivitusega, kuid see on juba rakendusliidesest sõltuv. Kahjuks reageerib SpeechRecognition liides sageli ka sõrmenipsudele, köhatustele, aevastustele, koputustele, plaksutustele, klaviatuuriklahvide vajutamisele ja muudele valjematele helidele, kuid ei suuda tuvastada sosistamist. Kuna inimkõnena tuvastatakse vääralt liiga palju muid helisid, mis eksami sooritamise ajal ruumis esineda võivad, saab väita, et antud kujul lahendus ei ole piisavalt täpne, et kontrollida ründeid, kus konsulteeritakse ruumis viibivate kõrvaliste isikutega või suheldakse kõneledes mõne seadme vahendusel.

6.2 Näotuvastus

Ruumis olevate nägude tuvastamiseks on proovitud kaht eri teenust: tracking.js [63] ja Kairos [64]. Näotuvastuse implementeerimise peamiseks eesmärgiks on teha kindlaks

ekraani ees viibivate isikute arv ning märgistada olukord, kui videovoos nägu puudub või neid esineb mitu. Kairose puhul on testitud ka kasutaja isikutuvastuse võimalusi.

6.2.1 Tracking.js

Tracking.js teek võimaldab veebilehitsejas kasutada reaalajalist raalnägemist (*computer vision*), et jälgida näiteks kaadris olevaid värve, objektide piirjooni ja nägusid [63]. Antud töö raames on katsetatud nägude avastamist veebikaamera videovoos. Programmikoodi (vt Joonis 23) aluseks on võetud tracking.js koodihoidlas olev näidis[1].

```
var canvas = document.getElementById('canvas');
var context = canvas.getContext('2d');
var objects = new tracking.ObjectTracker('face');

objects.setInitialScale(4);
objects.setStepSize(2);
objects.setEdgesDensity(0.1);

tracking.track('#video', objects, {camera: true});

objects.on('track', function (event) {
    context.clearRect(0, 0, canvas.width, canvas.height);

    event.data.forEach(function(rect) {
        context.strokeRect(rect.x, rect.y, rect.width, rect.height);
    });

    $('#numOfFacesTrackingJs').text(event.data.length);

    if (event.data.length > 1) {
        turnOverlayOn();
    }
});
```

Joonis 23. Tracking.js programmikood.

Kui kasutaja on andnud loa veebikaamera videovoo kasutamiseks, kuvatakse see HTMLi *canvas*-elemendil. Tracking.js tuvastab videovoost eelnevalt määratud objekti, milleks antud juhul on nägu, aga milleks võivad olla ka silmad või suu, ja kuvab veebirakenduse ülevaatlikus tabelis info kaadris olevate nägude arvu kohta. Jälgimise lihtsustamiseks joonistatakse nägude ümber ka nelinurgad. Kui nägusid on kaadris enam kui üks,

[1] https://github.com/eduardolundgren/tracking.js/blob/master/examples/face_camera.html

kuvatakse moodulaken (*turnOverlayOn()*), kus tuletatakse kasutajale meelde, et korraga võib arvuti ees viibida vaid üks isik.

Tracking.js teostab näoavastust pidevalt ja ajaliste piiranguteta. Intervalli kasutades on protsessi vajadusel võimalik teha perioodiliseks, näiteks kontrollida kasutajat iga viie sekundi tagant, kuid antud juhul on pidev info saamine kaadris viibivate nägude kohta isegi eelistatum. Kõige paremini tuvastas tracking.js töö raames tehtud katsetes nägu otsevaates või kergelt üles-alla suunatuna. Ka mitme otsevaates näo esinemist videokaadris määratakse tulemuslikult, eeldusel, et näod asuvad kaamerast vähemalt 1.5 meetri kaugusel. Positiivne on, et tracking.js tööd ei takista prillid ja nägu tuvastatakse edukalt ka siis, kui see on nähtaval vaid poolenisti.

Küll aga esineb tracking.js töös mõningaid ebatäpsusi. Nägu ei tuvastata, kui pea on ekraanist ligikaudu 40-kraadise nurga all eemale või 20-kraadise nurga all küljele pööratud. Mõnikord tuvastatakse kirju tausta korral kaadris rohkem nägusid, kui seal tegelikult on. Samuti on raskusi näotuvastusega, kui näod ei asu kaamerale piisavalt lähedal või on osaliselt varjatud juustega, näiteks tukaga. Kõige paremad tulemused on päevavalguses, kui töölaud on paigutatud nii, et kasutaja on näoga akna poole.

Eelnevast tulenevalt võib väita, et tracking.js teek oleks sobilik algeliseks näoavastuseks eksami järelevalve kaitsesüsteemis, võimaldades loendada kaadris esinevaid nägusid. Küll aga ei ole tegemist lõplikult usaldusväärse lahendusega, kuna avastusprotsessis esineb sageli vigu. Lisaks ei võimalda tracking.js tuvastada näo abil kasutaja isikut, et kontrollida eksamikandidaatide vahetumist testi sooritamise jooksul.

6.2.2 Kairos

Kairos pakub mitmeid erinevaid näotuvastuse rakendusi alates näoavastusest ja emotsioonide määramisest kuni kasutaja autentimiseni nii staatilisi fotosid kui dünaamilisi videoid kasutades [64]. Kairosel on isiklikuks kasutamiseks tasuta REST-rakendusliides ja spetsiaalne JavaScript'i teek[1]. Tasuta versiooni puhul kehtib piirang 25 päringut minutis ja kuni 1500 päringut päevas, mistõttu on see kasutatav peamise funktsionaalsuse testimiseks, kuid mitte lõpliku lahenduse loomiseks.

[1] https://github.com/kairosinc/Kairos-SDK-Javascript

Kairost on lihtne kasutada − piisab vaid pildifaili edastamisest rakendusliidesele, mis tagastab JSON-formaadis andmed fotol oleva näo kohta. Antud töö raames koostatud veebirakenduses on Kairosele edastatud base64-formaadis andmed HTMLi *canvas*-elemendile projitseeritud veebikaamera videovoo stoppkaadrist (vt Joonis 24). Kuna mõningad Kairose rakendusliidese päringud, näiteks emotsioonide analüüs, aktsepteerivad meediaobjekti vaid URLi või faili kujul, ei ole antud testis neid kasutatud.

```
function getImageFromCanvas() {
    var context = canvas.getContext('2d');
    context.drawImage(video, 0, 0, kairosWidth, kairosHeight);
    return canvas.toDataURL('image/png');
}
```

Joonis 24. Kairose rakendusliidese jaoks sobivas formaadis pildifaili saamine.

Küll aga sobib veebirakenduse koostatav pildiformaat paljudele teistele Kairose päringutele (vt Tabel 5). Näiteks tagastab *detect*-päring rakendusliidesele fotot saates info kaadris olevate nägude kohta, sealhulgas lõua ja silmade asukoha, peaasendi, prillide olemasolu, isiku soo, eeldatava vanuse ja rassilise kuuluvuse [65]. Kui kaadris inimnägusid pole, tagastatakse vastav veateade („*no faces found in the image*“). *Detect*-meetod ei salvesta ega kontrolli kasutaja isikut, mistõttu ei ole ta piisavalt täpne kasutaja autentimiseks. Küll aga toetab *detect*-päringu vastusena saadav kergbiomeetriline info (kasutaja rass, sugu, nägemisabivahendite kasutamine ja vanus) kasutaja pidevtuvastamist, võimaldades reageerida kasutaja vahetumisele viitavatele muutustele. Eelkõige saaks kontrollida eksaminandi sugu ja rassi. Prillide kasutamise põhjal lõplikku otsust langetada ei saa, kuna testi tegemise ajal ei ole välistatud prillide eemaldamine. Samuti sõltub kasutajale määratud vanus näoilmest, peaasendist või valgustatusest, mistõttu oleks vanuse puhul mõistlik tuvastada vaid olukorrad, kus registreerumisel esitatud vanus erineb Kairose hinnangulisest vanusest vähemalt kümme aastat.

Tabel 5. Vasted Kairose päringutele kaadris olevate nägude arvust sõltuvalt.

Päring	**Kaadris pole nägusid**	**Kaadris on üks nägu**	**Kaadris on mitu nägu**
detect	„*no faces found in the image*“	tagastab näo info (peaasend, sugu, rass, vanus, prillid)	tagastab iga näo info (peaasend, sugu, rass, vanus, prillid)
enroll	„*no faces found in the image*“	salvestab ja tagastab näo info (peaasend, sugu, rass, vanus, prillid)	salvestab ja tagastab iga näo info (peaasend, sugu, rass, vanus, prillid) või „*too many faces in image*“
recognize	„*no faces found in the image*“	tagastab potentsiaalsed vasted galeriisse salvestatud nägude seast või „*no match found*“	tagastab potentsiaalsed vasted galeriisse salvestatud nägude seast või „*no match found*“
verify	„*no faces found in the image*“	tagastab kõige täpsema vaste galeriisse salvestatud nägude seast või „*no match found*“	„*too many faces in image*“

Enroll salvestab kaadris oleva näo Kairose ajutisse andmebaasi (edaspidi ka galerii), kasutades selleks lisatud inimest iseloomustavat identifikaatorit (*subject_id*), ja tagastab ühtlasi info kaadris oleva näo kohta (sugu, rass, prillid, vanus, huulte ja pea asend), galeriisse lisamise ajatempli, galerii nime ja nägu iseloomustava identifikaatori (*face_id*) [65]. Galeriisse salvestatud nägude põhjal on hiljem võimalik kasutajaid tuvastada. Kairose dokumentatsiooni sõnul on tuvastus optimaalne, kui isikust on galeriisse salvestatud 6−8 pilti, kuid tuvastus töötab edukalt ka ainult ühe foto olemasolul. Kuna lisaks isiku salvestamisele galeriisse tagastab *enroll*-meetod ka kergbiomeetrilist infot kaadris viibiva isiku kohta, on kasutaja pidevtuvastuse toetamiseks mõistlikum kasutada *enroll*-i kui *detect*-i. Samuti kontrollib *enroll* vaikimisi, et kaadris viibiks vaid üks isik, kuigi vajadusel on seda võimalik muuta.

Antud töö raames koostatud veebirakenduses on kasutaja galeriisse lisamine lahendatud veebilehe avamise hetkel. Esmalt kustutatakse galerii selle varasema olemasolu korral, et välistada aegunud info kasutamist. Seejärel kuvatakse kasutajale veebilehele navigeerides moodulaken, mis küsib tema meiliaadressi, millest saab kasutaja identifikaator (*subject_id*) kaitsesüsteemis. Sisselogimisnupule vajutades käivitatakse *enroll*-päringu väljakutse, mis loob ühtlasi uue galerii, ning kasutaja nägu ja meiliaadress seotakse omavahel. Edaspidi on salvestatud andmeid võimalik kasutada kandidaadi

otsimiseks galeriist nii identifikaatori kui ka näo põhjal. Esimesel juhul tuleb kasutada *verify*- ja teisel juhul *recognize*-päringu väljakutset. Reaalsuses oleks loomulikult lisaks meiliaadressile tarvilik kontrollida ka kasutaja salasõna.

Recognize-päring leiab eelnevalt loodud galeriis olevatest nägudest sellised, mis vastavad kaadris olevatele, ja tagastab need koos nägusid ja isikuid iseloomustavate identifikaatorite, galeriisse salvestamise ajatempli ja täpsuskvoodiga [65]. Kui galeriisse on salvestatud mitu kaadris olevat isikut, tagastab *recognize*-päring info iga tuvastatud isiku kohta. Kui kaadris on mitu nägu, millest üks on galeriis registreeritud kandidaadi oma, tagastatakse tolle vaste. Vaikimisi tagastatakse vasted, mille sarnasus kaadris oleva isikuga on vähemalt 60%, kuid antud parameetrit on võimalik vastavalt vajadusele muuta. Käesoleva töö raames tehtud katsed näitasid, et sobilik limiit võib edukaks tuvastuseks olla isegi 80%, eeldusel, et sisseastumistesti lahendades on kasutaja enamasti näoga arvutiekraani poole suunatud, muutes peaasendit vaid klaviatuuri vaatamiseks. Kõige enam mõjutavad tuvastamise edukust näo osaline varjamine (eelkõige nina, suu või mõlema silma), prillide eemaldamine ja ekraanist liigselt eemale suunatud peaasend (eelkõige külgede suunas).

Kui nägusid kaadris pole või kui kaadris olevad isikud ei sarnane ühelegi eelnevalt galeriisse lisatud isikule piisaval määral, tagastatakse veateade (vastavalt „*no faces found in the image*“ ja „*no match found*“). Järelikult on *recognize*-päringu abil võimalik tuvastada galeriisse lisatud inimesi ja seda, kas parasjagu kaamera ees viibiv isik on varasemalt salvestatud (*enroll*) või on tegemist variisikuga. Teisalt puudub võimalus kontrollida kaadris olevate isikute koguarvu, eeldusel, et ainult üks neist on galeriisse lisatud.

Verify-päringu eesmärgiks on kinnitada, et kaadris olev isik vastab konkreetsele galeriist küsitud isikule [65]. Selleks edastatakse rakendusliidesele veebikaamera stoppkaader ja tuvastatava isiku identifikaator (*subject_id* ehk registreerumisel salvestatud meiliaadress). Kui kaadris viibiv isik vastab konkreetsele andmebaasi salvestatud isikule, tagastatakse nägu iseloomustav identifikaator (*face_id*) ja täpsushinnang. Tuvastuse edukust mõjutab taaskord näo olulisemate tunnusjoonte varjamine, kuid peaasendi suhtes tundub liides vähem piirav olevat.

Antud töö raames Kairosega tehtud katsed sooritati kohas, kus osalejad istusid näoga päevavalguse poole. Osalejate peaasend ei olnud fikseeritud. Sarnasemaks muutmiseks kasutati vajadusel käepäraseid vahendeid, nagu klambrid, peavõru või prillid, kuid ei kasutatud meiki ega parukaid. Sarnasuskvoodi puhul on edaspidi esitatud katsete kõrgeim tulemus kui rakendusliidese vastustele seatava minimaalse piiri soovitus, kusjuures sarnasuskvoot näitab, kui suure tõenäosusega peeti teisi isikuid galeriisse salvestatud osalejaga samaks isikuks.

Ühes kontrollkatses osalesid kaks sarnaste näojoontega eri soost isikut, mõlemal heledad juuksed, nägemist parandavad prillid ja sarnased kulmud. Naine lisati galeriisse prille kandes, meest galeriisse ei lisatud. *Verify*-päringus peeti meest naiseks kindlusega 0.4456, kui ta kandis naise prille, tõenäosusega 0.3518 oma prille kandes ja ilma prillideta 0.3070 (vt Tabel 6). Katset korrati ilma prillideta ja tekitades mõlemal laubale tuka, üritades välimusi veelgi sarnasemaks muuta. Baasväärtuseks võeti kummaski katses olukord, kus naist võrreldi iseendaga.

Tabel 6. Sarnasuse katse eri soost isikutega.

Tüüp	**Naine (registreeritud)**	**Mees (registreerimata)**	**Sarnasus (kõrgeim tulemus)**
1	naise prillid	–	0.9903
	naise prillid	naise prillid	0.4456
	naise prillid	mehe prillid	0.3518
	naise prillid	ilma prillideta	0.3070
2	ilma prillideta, tukaga	–	0.9866
	ilma prillideta, tukaga	ilma prillideta, tukaga	0.2954
	ilma prillideta, tukaga	ilma prillideta, ilma tukata	0.3268

Rakendusliidest testiti ka naissoost ühe munaraku kaksikutega, et teha kindlaks, kui hästi Kairos neid eristab (vt Tabel 7). Eri kaksikuid hinnati sarnasemaks, kui mõlemad kandsid samu prille. Ilma prillideta suutis rakendus kaksikutel paremini vahet teha. Katsest ilmnes, et ainult prillide abil sarnasemaks muudetud kaksikuid peeti samaks isikuks lausa üle 80% tõenäosusega, millest on võimalik järeldada, et kaksikute variisikuna esinemise takistamiseks peaks isikute eristamiseks määratud piir olema tollest kõrgem.

Tabel 7. Sarnasuse katse ühe munaraku kaksikutega.

Tüüp	**Väljakutse**	**Registreeritud isik (*enroll*)**	**Kontrollisik**	**Sarnasus (kõrgeim tulemus)**
1 (prillidega)	recognize	A	A	0.9701
	verify	A	A	0.9662
	recognize	A	B	0.8028
	verify	A	B	0.8483
2 (ilma prillideta)	recognize	B	B	0.9805
	verify	B	B	0.9834
	recognize	B	A	0.7697
	verify	B	A	0.7932

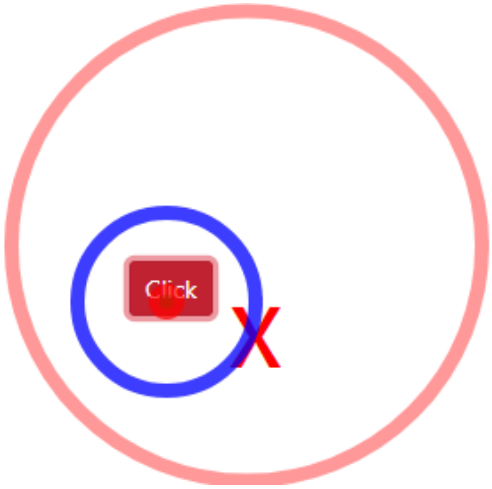
Kairose rakendusliidesega tehtud katsetustest järeldub, et kuigi tasuta versiooni päringute arv on piiratud, võiks kaaluda täisversiooni kasutamist näotuvastuse implementeerimiseks sisseastumistesti kaitsesüsteemis. Registreerumisel saaks *enroll*-meetodit kasutades andmebaasi salvestada nii kandidaadi dokumendifoto kui ka tema hetkelise näopildi, mille alusel hiljem *verify*-päringut kasutades isikut kontrollida. Küll aga tuleb tähele panna, et olukorras, kus galeriisse on salvestatud ainult dokumendifoto, on videovoos oleva näo vastavus dokumendifotole väiksem (katsetes ligikaudu 60−70%), mistõttu tuleks igal sisselogimisel kandidaadi veebikaameralt saadav näopilt uuesti registreerida ning ühtlasi eelnevatega võrrelda. Samuti tasub igal süsteemi sisenemisel *enroll*-päringuga tuvastada kergbiomeetrilised andmed ja neid süsteemi kasutamise ajal *detect*- või *enroll*-meetodi abil jälgida. Kaadris olevate isikute arvu määramiseks ja kandidaadi isiku pidevtuvastuse teostamiseks tuleks kasutada *verify*-väljakutset, millele on rakendatud piirang, mis lubab kaadris olla vaid ühel näol. *Recognize*-päringut oleks mõistlik kasutada, takistamaks olukorda, kus testi lahendamise ajal viibib arvuti ees kaks või enam sisseastujat, kes on mõlemad galeriisse salvestatud, kuid kuna autori hinnangul on mitme näo esinemine juba kaetud *verify*-ga, pole antud meetodi kasutamine tarvilik.

Kahe näotuvastuslahenduse tracking.js ja Kairose võrdlusest on näha, et Kairose rakendusliides on rohkemate võimalustega ja suurema paindlikkusega, mistõttu tasub neist kahest eelistada just seda.

6.3 Silmade liikumine

Viimasena uuriti põgusalt xLabs pea- ja pilgujälgimislahendust [66], et teha kindlaks, kas too oleks sobilik veebikaamera vahendusel kasutaja silmade fookuspunkti määramiseks. xLabs'i kasutamiseks on vajalik Chrome'i veebilehitseja plugin ja veebikaamera [67].

Esmalt tuleb pilgujälgija kalibreerida [67]. Selleks piisab erinevaid ekraanipunkte vaadates fookuskohas hiirekliki tegemisest. Testrakenduses on see lahendatud nupu abil, mis vajutades muudab oma asukohta ekraanil (vt Joonis 25). Enamasti piisab esmaseks kalibreerimiseks 8−15 kordusest, kuid mida enam vajutusi ja mida laiemal pinnal, seda täpsem tulemus.



Joonis 25. xLabs kalibreerimine testrakenduses. Sinise ringiga ümbritsetud punane ring tähistab hiirekliki toimumise asukohta, punane X ja roosa ring viitavad pilgu fookuspunktile, kusjuures xLab'i roosa ringi visualisatsioon liigub suurema viivitusega kui testrakenduse X.

Kuigi xLabs'i kasutades ei ole kohustust peaasendit fikseerida [66], võtab sageli muutuva peaasendi korral edukas kalibreerimine kauem aega ning tulemus on ebatäpsem kui enam-vähem staatilise poosi korral. Üldiselt liiguvad nii xLabs'i enda pilgupunkti visualisatsioon kui ka rakendusliideselt saadavate koordinaatide järgi paigutatav testrakenduse sümbol tegeliku pilgupunktiga arvestatavalt heas kooskõlas, eriti, kui kalibreerida põhjalikumalt ja pead paigal hoides. Katsetes aga tekkis visualisatsioonides viivitus, mistõttu nupu asukoha muutudes ekraanil jõuti uude punkti esmalt liikuda siiski kursoriga, kui pilgutähis silmade uuest fookusest märku andis.

Kõige parem on xLabs'i kasutada, kui nägu valgustab ühtlaselt päevavalgus [67]. Hämaras on pilgutuvastus raskendatud. Kahjuks ei ole xLabs võimeline läbi prilliklaaside

pilku jälgima, mis võib osutuda takistuseks neile, kel on ilma korrigeerivate vahenditeta raskusi arvutiekraanil oleva nägemisega.

Lisaks tuvastab xLabs edukalt mitme ekraani olemasolu ning kuvab plugina seadete lehel teate, et välise ekraaniga lahendus ei tööta, kuid praktilised katsed näitasid, et tegelikult on jälgimist võimalik kasutada ka siis, kui sülearvutiga on ühendatud mitu ekraani.

Võrreldes professionaalse lahendusega (Tobii Pro) on xLabs'il veel arenguruumi, kuid on positiivne, et eksisteerib variant, mille puhul ei ole kasutaja liikumine piiratud ja mis võimaldab pilku jälgida vaid veebikaamerat kasutades. Kindlasti tasub xLabs'i ja analoogseid rakendusi kasutada veebipõhiste testide järelevalve teostamise toetamiseks. Antud töö skoopi arvesse võttes ei ole pilgujälgimist käepäraste vahenditega implementeeritud. See, kuidas võiks xLabs'i kasutada RangeForce kontekstis, vajab edasist uurimist.

7 Küberkaitse eriala sisseastumistesti jaoks sobiva süsteemi kirjeldus

Käesolevas peatükis kirjeldatakse Tallinna Tehnikaülikooli küberkaitse eriala sisseastumistesti kaitsesüsteemi üldist toimimist, võttes arvesse eelpool esitatud ründeid, võimalikke kaitsemeetmeid, varasemalt tehtud töid ning praktiliste katsetuste tulemusi. Süsteemi funktsionaalsed ja mittefunktsionaalsed nõuded on esitatud lisas 4.

Tegemist on klient-server lahendusega, mis jaguneb üldpildis kaheks. Kandidaadi arvutisse paigaldatava programmi näol on sisuliselt tegemist lukustusbrauseriga. Programmi käivitudes blokeeritakse lokaalses masinas võimalused avada teisi rakendusi, sealhulgas klahvikombinatsioonide (nagu Ctrl+Alt+Del) abil kaitsesüsteemi sulgedes. Tänu sellele on takistatud keelatud abivahendite kasutamine kandidaadi arvutis. Rakenduse avamisel kontrollitakse lisaekraanide olemasolu ning seda, kas rakendus käivitati virtuaalmasinas, mispuhul rakendus teavitab kasutajat tingimuste rikkumisest ja sulgub.

Lukustusbrauseri edukal käivitumisel palutakse kasutajalt autentimist. Kui kandidaadil kasutajakontot ei ole, on esitatud võimalus see luua. Konto luuakse kandidaadi meiliaadressi, ees- ja perekonnanime alusel, hõlbustamaks sidumist ülikooli sisseastumisi haldava süsteemiga. Lisaks nõutakse kandidaadilt pildiga isikut tõendava dokumendi esitamist, kusjuures dokumendifoto on hiljem aluseks näotuvastusele. Eduka sisselogimise korral palutakse kandidaadil salvestada video, mis annab põhjaliku 360-kraadise ülevaate keskkonnast, kus sisseastumistesti sooritatakse, ning suunatakse kandidaat RangeForce keskkonda, kus tal on võimalik sooritada sisseastumistesti laboreid. Samal ajal hakkab tööle kasutaja pidevtuvastus, mis jälgib kogu süsteemi lahti oleku ajal veebikaamera, sisendseadmete (klaviatuur, hiir) ja mikrofoni abil kasutaja nägu, trükkimise dünaamikat, hiire kasutusviisi ja riiete värvi, tuvastamaks kehastusründe esinemist. Välise abi kasutamist kontrollitakse silmade fookuspunkti, ruumiheli ja ruumist esinevat videovoogu jälgides. Seansi jooksul edastatakse kogutud andmed serverile, kus toimub nende salvestus ja analüüs.

Igale kandidaadile on määratud usalduskvoot, mis on süsteemi sisenedes 100%. See tähendab, et süsteemi sisenemise hetkel eeldatakse, et kandidaat ei riku eksamikorda. Kui kaitsesüsteem tuvastab eksamikorra rikkumise, märgistab ta antud koha salvestatud videos ning vähendab kandidaadi usalduskvooti. Kindlat piiri, millest allapoole langedes takistatakse kandidaadil sisseastumistestide sooritamist, ei ole, kuid usalduskvoot kuvatakse hiljem kandidaadi soorituse kohta käivate andmete juures ning ülikooli esindajal on sellele vastavalt võimalik teha otsus sisseastumistesti läbimise kohta. Kuna eksamikorra rikkumise vastane kaitsesüsteem alustab aktiivselt tööd sisse logimise hetkest, on oluline, et kandidaat tegeleks rakenduse tööl oleku ajal ainult sisseastumistesti lahendamisega. Seetõttu tuleb kandidaati kindlasti enne sisse logimist informeerida eksamikorrast ja tingimustest. Kui kandidaat soovib sisseastumistesti hiljem jätkata, on võimalik andmete kogumine lõpetada ja kaitsesüsteem sulgeda sellest välja logides.

Ülikooli esindajale mõeldud alamosa võimaldab sisseastumistesti veebirakenduse vahendusel hallata. Esindaja sisse logides kuvatakse rakenduse avalehel nimekiri lisakontrolli vajavatest testitulemustest ehk nendest sooritustest, mis jäävad allapoole teatud piiri, mille ülikool on kandidaadi usalduskvoodile määranud. Läbimispiiri on ülikoolil võimalik jooksvalt muuta. Iga sooritusе juures on välja toodud videosalvestus kogu sooritusest, kusjuures süsteemi poolt eksamikorra rikkumisena tuvastatud hetked on eraldi märgistatud, hõlbustades nendeni navigeerimist ja nende manuaalset kontrolli. Sooritуste manuaalne üle vaatamine ei ole vajalik, aga on soovi korral võimalik. Lisaks on veebirakenduses kõigi kaitsesüsteemiga liitunud kandidaatide nimekirja sisaldav alamleht. Nimekirja ja otsingu kaudu on võimalik navigeerida iga kandidaadi individuaalsele profiilile, kus on esitatud usalduskvoodi keskmine, andmed kandidaadi kohta (sealhulgas fotojäädvustus isikut tõendavast dokumendist) ning viited kaitsesüsteemiga tehtud sisseastumistesti laborite sooritustele koos märgistatud videolindistustega. Kui usalduskvoot on liiga madal, on ülikooli esindajal intervjuuvoorus võimalik küsida täpsustavaid küsimusi sisseastumistesti sooritamise kohta.

Kaitsesüsteemiks on kandidaadi arvutisse installitav rakendus, kuna nii on kõige suurem kontroll lokaalses masinas toimuva üle. Veebiplugina või -rakenduse kasutamine ei ole antud ülesandepüstituse puhul piisav, kuna ei võimalda blokeerida lokaalses masinas avatavaid rakendusi. Oluline on, et sisseastumistesti järelevalvega lahendamiseks ei oleks kandidaadil vaja eririistvara. Välja pakutud süsteemi korral on oluline vaid arvuti,

klaviatuuri, hiire, veebikaamera, mikrofoni ja kõlarite olemasolu ning puudub vajadus spetsiaalse välise järelevalveseadme ostmiseks.

Klient-server arhitektuuri kasuks otsustati lootuses, et nii on kandidaadil vähem võimalusi kaitsesüsteemi toimimisele vahele segada, selle töötamispõhimõtteid muuta ja niiviisi ülikoolile valeinfot edastada. Samas tuleb tõdeda, et ükski programm ei ole kunagi kõigi rünnete eest kaitstud. Lisaks andmeanalüüsiga tegeleva süsteemi kaitsmisele vähendab klient-serveri arhitektuur kandidaadi arvuti koormust, teostades isikutuvastuseks ja andmeanalüüsiks vajalikud operatsioonid ülikooli kui teenusepakkuja ressursse kasutades.

Välja pakutud lahendusel on kaks probleemset kohta. Eksamikeskkonna korrektsuse hindamine eeldab hetkel ruumist ülevaate andva video lindistamist, kuid miski ei takista kandidaadil pärast video lindistamist mõnest peidukohast abimaterjale taas välja võtta. Selleks, et saada ruumist täielikku ülevaadet, tuleb kandidaadile väga selgelt kommunikeerida, mida video endas sisaldama peab (lagi, põrand, seinad, töölaud, lauaalune). Kuna ruumi sobivuse kontroll ei toimu reaalajas, tekib küsimus, kuidas mõjutab hinnangut kandidaadi sooritusele see, kui lindistatud video või selles nähtav keskkond ei vasta sisseastumistesti nõuetele. Lahenduseks oleks reaalajalise kontrolli implementeerimine, kuid kuna see nõuaks inimressursi kättesaadavust, piiraks see eksami sooritamise paindlikkust, nõuaks nii vaatlejalt kui kandidaadilt planeerimist ja takistaks testi tegemist kandidaadile sobival ajal. Kuigi ka eellindistatud videote vaatamiseks on vajalik inimfaktor, on salvestisi võimalik järele vaadata mitme kaupa ja kiirendatult.

Teiseks probleemiks on andmeühenduse kiirus. Serverile on vaja edastada nii videot kui ka sisendseadmetelt saadavaid andmeid, mille pidev ülekanne serveripoolele koormab ühendust. Üheks võimalikult lahenduseks oleks andmete perioodiline edastamine, see tähendab, et video puhul ei edastataks mitte kogu videot, vaid teatud ajavahemike tagant tehtud kaadreid. Võib eeldada, et piisavalt väikese ajaraami (nt 2 sekundit) puhul ei jõua eksamikorra rikkumise koha pealt midagi kriitilist juhtuda. Teisalt, kuna videot ei kontrollita ning kandidaadile ei anta eksamikorra rikkumise kohta tagasisidet reaalajas, ei ole oluline ka selle momentne jõudmine serverisse, mistõttu on võimalik taustaprotsessina videot serverile edastada aeglasemalt, kui seda filmitakse. Video edastamine võib isegi edasi kesta pärast kaitsesüsteemi sulgemist või jätkuda pärast kaitsesüsteemi taasavamist. Sellise lahenduse puhul jõuab serverisse kogu andmestik.

8 Kokkuvõte

Käesoleva töö eesmärkideks oli katsetada mõningaid võimalusi veebipõhiste testide rikkumatuse tagamiseks, tuvastada TTÜ küberkaitse eriala sisseastumistesti jaoks sobivad kaitsemeetmed ning koostada nende baasil kaitsesüsteemi esmane analüüs. Eesmärkide saavutamiseks koostati ründestsenaariume kirjeldav ründe-kaitsepuu, uuriti võimalikke lahendusi kasutaja pidevtuvastuseks ja kõrvalise abi kasutamise avastamiseks ning teostati katseid, kasutades nii käepäraseid vahendeid, nagu sülearvuti integreeritud mikrofon ja veebikaamera, kui ka spetsiaalselt riistvara.

Pilgujälgimiskatse tulemusena ilmnes, et eririistvaraline lahendus suudab silmade fookuspunkti jälgida paremini kui veebikaamerale mõeldu. Jõuti järeldusele, et erinevalt miimikast ei anna silmade liikumine piisavalt infot kasutatava keskkonna (RangeForce, Youtube, Postimees) üheseks määramiseks, kuid selle alusel saab kindlaks teha, kas vaadatakse tekstilist või graafilist sisu. Hiire ja pilgu liikumise järjekorra analüüs võimaldab tuvastada, kas kasutaja sooritab tegevusi ise või jälgib toimuvat lisaekraani vahendusel. Samuti selgus, et terminalikäskude sisestamiseks kasutatakse erinevaid trükkimise, kopeerimise ja kleepimise kombinatsioone.

Teises katses tõestati, et algelise kaitsesüsteemi implementeerimiseks on võimalik kasutada mõningaid olemasolevaid JavaScripti teeke. Eriti hästi töötas Kairose näotuvastuslahendus, samas esines puudujääke ruumihelist inimkõne eristamisel. Kinnitati, et ka tavalise veebikaameraga on võimalik jälgida silmade liikumist, kuigi nii on tulemus ebatäpsem kui eririistvaralise seadme korral.

Kuigi töö tulemusena on esitatud TTÜ küberkaitse eriala sisseastumistesti kaitsesüsteemi kirjeldus ja nõuded, on tööd võimalik aluseks võtta ka muude veebipõhiste keskkondade, kus kasutaja pidevtuvastus on oluline, turvasüsteemide välja töötamiseks. Antud töö loodab lisaks TTÜ küberkaitse eriala sisseastumistesti kaitsesüsteemi implementeerimise lubamisele võimaldada ka muude veebipõhist interaktsiooni vajavate protsesside rikkumatuse tagamist.

Kasutatud kirjandus

[1] "e-Teatmik: IT ja sidetehnika seletav sõnaraamat." [Online]. Available: http://vallaste.ee/. [Accessed: 03-Apr-2018].

[2] ITIL, "DevOps Glossary English-Estonian." 2017.

[3] W. Louis, M. Komeili, and D. Hatzinakos, "Continuous authentication using One-Dimensional Multi-Resolution Local Binary Patterns (1DMRLBP) in ECG biometrics," *IEEE Trans. Inf. Forensics Secur.*, 2016.

[4] Webopedia, "What is equal error rate (EER)?" [Online]. Available: https://www.webopedia.com/TERM/E/equal_error_rate.html. [Accessed: 04-Apr-2018].

[5] Y. Matsuyama, M. Shozawa, and R. Yokote, "Brain signal′s low-frequency fits the continuous authentication," *Neurocomputing*, vol. 164, pp. 137–143, Sep. 2015.

[6] AS Eesti Meedia, "Tervisenõustamise keskkond - Kliinik.ee." [Online]. Available: https://www.kliinik.ee/. [Accessed: 03-Apr-2018].

[7] Eesti Keele Instituut, "Eesti õigekeelsussõnaraamat ÕS 2013." [Online]. Available: http://www.eki.ee/dict/qs/. [Accessed: 03-Apr-2018].

[8] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "DeepFace: Closing the Gap to Human-Level Performance in Face Verification," in *2014 IEEE Conference on Computer Vision and Pattern Recognition*, 2014, pp. 1701–1708.

[9] "What is an LMS. What LMS means. Definition of a Learning Management System." [Online]. Available: https://www.easy-lms.com/help/lms-knowledge-center/what-is-an-lms/item10182. [Accessed: 03-Apr-2018].

[10] IMS Global Learning Consortium, "Learning Tools Interoperability." [Online]. Available: https://www.imsglobal.org/activity/learning-tools-interoperability. [Accessed: 12-Feb-2018].

[11] I. Traoré, Y. Nakkabi, S. Saad, B. Sayed, J. D. Ardigo, and P. M. De Faria Quinan, "Ensuring online exam integrity through continuous biometric authentication," in *Information Security Practices: Emerging Threats and Perspectives*, 2017.

[12] A. M. Kaplan and M. Haenlein, "Higher education and the digital revolution: About MOOCs, SPOCs, social media, and the Cookie Monster," *Bus. Horiz.*, vol. 59, no. 4, pp. 441–450, Jul. 2016.

[13] Tartu Ülikool, "MOOCid." [Online]. Available: https://www.ut.ee/et/oppimine/moocid. [Accessed: 03-Apr-2018].

[14] J. Daugman, "How Iris Recognition Works," in *The Essential Guide to Image Processing*, Elsevier, 2009, pp. 715–739.

[15] V. Korrovits and H. Käämbre, "Inglise-eesti füüsika sõnaraamat." [Online]. Available: http://www.keeleveeb.ee/dict/speciality/physics_enet/. [Accessed: 03-Apr-2018].

[16] Cybernetica AS, “AKIT - Andmekaitse ja infoturbe leksikon.” [Online]. Available: https://akit.cyber.ee/. [Accessed: 09-Apr-2018].

[17] B. Kordy, S. Mauw, S. Radomirović, and P. Schweitzer, “Foundations of Attack–Defense Trees,” in *Formal Aspects of Security and Trust*, Springer, Berlin, Heidelberg, 2011, pp. 80–95.

[18] V. Kiisk, “Spektroskoopia alused (loengukonspekt).” Tartu, 2017.

[19] Eesti Keele Instituut., “Eesti keele seletav sõnaraamat,” 2009. [Online]. Available: http://www.eki.ee/dict/ekss/ekss.html. [Accessed: 03-Apr-2018].

[20] H. Corrigan-Gibbs, N. Gupta, C. Northcutt, E. Cutrell, and W. Thies, “Deterring Cheating in Online Environments,” *ACM Trans. Comput. Interact.*, 2015.

[21] “TTÜ õppeinfosüsteem.” [Online]. Available: https://ois2.ttu.ee/uusois/uus_ois2.tud_leht. [Accessed: 26-Mar-2018].

[22] “Küberkaitse.” [Online]. Available: https://www.ttu.ee/teaduskond/infotehnoloogia-teaduskond/sisseastujale-34/magistriope-50/kuberkaitse-2/. [Accessed: 26-Mar-2018].

[23] “Küberkaitse.” [Online]. Available: https://www.ttu.ee/sisseastujale/magistriope-2/23289/sisseastumiskatsed/lisainfo/kuberkaitse-5/. [Accessed: 26-Mar-2018].

[24] “Rangeforce.” [Online]. Available: https://rangeforce.com/home. [Accessed: 26-Mar-2018].

[25] M. Ernits and K. Kikkas, “A Live Virtual Simulator for Teaching Cybersecurity to Information Technology Students,” in *Zaphiris P., Ioannou A. (eds) Learning and Collaboration Technologies. LCT 2016. Lecture Notes in Computer Science, vol 9753*, Springer, Cham, 2016, pp. 474–486.

[26] A. Fask, F. Englander, and Z. Wang, “Do Online Exams Facilitate Cheating? An Experiment Designed to Separate Possible Cheating from the Effect of the Online Test Taking Environment,” *J. Acad. Ethics*, vol. 12, no. 2, 2014.

[27] O. R. Harmon and J. Lambrinos, “Are online exams an invitation to cheat?,” *J. Econ. Educ.*, 2008.

[28] H. M. Alessio, N. Malay, K. Maurer, A. J. Bailer, and B. Rubin, “Examining the Effect of Proctoring on Online Test Scores,” *Online Learn.*, vol. 21, no. 1, 2017.

[29] G. Sindre and A. Vegendla, “E - exams versus paper exams : A comparative analysis of cheating - related security threats and countermeasures.”

[30] R. Bawarith, A. Basuhail, A. Fattouh, and S. Gamalel-Din, “E-exam Cheating Detection System,” *IJACSA) Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 4, 2017.

[31] C. Y. Chuang, S. D. Craig, and J. Femiani, “Detecting probable cheating during online assessments based on time delay and head pose,” *High. Educ. Res. Dev.*, vol. 36, no. 6, pp. 1123–1137, Sep. 2017.

[32] W. A. Rosen and M. E. Carr, “An autonomous articulating desktop robot for proctoring remote online examinations,” in *2013 IEEE Frontiers in Education Conference (FIE)*, 2013, pp. 1935–1939.

[33] Y. Atoum, L. Chen, A. X. Liu, S. D. H. Hsu, and X. Liu, “Automated Online Exam Proctoring,” *IEEE Trans. Multimed.*, 2017.

[34] G. Fenu, M. Marras, and L. Boratto, “A multi-biometric system for continuous student authentication in e-learning platforms,” *Pattern Recognit. Lett.*, Apr. 2017.

[35] N. L. Clarke, P. Dowland, and S. M. Furnell, “e-Invigilator: A Biometric-Based Supervision System for e-Assessments,” in *International Conference on Information Society (i-Society), 2013*, 2013, p. 5.

[36] A. Amigud, J. Arnedo-Moreno, T. Daradoumis, and A.-E. Guerrero-Roldan, “Using Learning Analytics for Preserving Academic Integrity,” *Int. Rev. Res. Open Distrib. Learn.*, 2017.

[37] U. K. Mothukuri, S. Jain, and V. Muralidharan, “Invigilated online assessment: Various ways to minimize unauthorized help,” in *2012 IEEE Symposium on E-Learning, E-Management and E-Services, IS3e 2012*, 2012, pp. 35–38.

[38] M. C. Carlisle and L. C. Baird, “Design and use of a secure testing environment on untrusted hardware,” in *Proceedings of the 2007 IEEE Workshop on Information Assurance, IAW*, 2007.

[39] M. Lilley, J. Meere, and T. Barker, “Remote Live Invigilation: A Pilot Study,” *J. Interact. Media Educ.*, vol. 2016, no. 1, Jan. 2016.

[40] Software Secure, “Eyes on Integrity. A Comparative Look at Online Proctoring Models.” 2016.

[41] Pearson Education Inc, “Testing outside a test center.” [Online]. Available: https://home.pearsonvue.com/Test-Owner/Deliver-your-exam/Testing-outside-a-test-center.aspx. [Accessed: 12-Feb-2018].

[42] S. Jose, “Online Proctoring is Trending: Here is All You Should Know About It.” [Online]. Available: http://blog.talview.com/a-complete-guide-to-online-remote-proctoring. [Accessed: 09-Feb-2018].

[43] Software Secure, “RPNow Online Proctoring - Secure Testing. Anytime. Anywhere.” [Online]. Available: http://www.softwaresecure.com/product/remote-proctor-now/. [Accessed: 12-Feb-2018].

[44] “Talview Cognitive Video Interviewing - Video Interview Software.” [Online]. Available: https://talview.com/. [Accessed: 08-May-2018].

[45] B. Schneier, “Attack Trees,” in *Secrets and Lies*, Indianapolis, Indiana: Wiley Publishing, Inc., 2015, pp. 318–333.

[46] “ADTool.” [Online]. Available: http://satoss.uni.lu/members/piotr/adtool/. [Accessed: 11-Apr-2018].

[47] J. D. Woodward, C. Horn, J. Gatune, and A. Thomas, “Biometrics. A Look at Facial Recognition.” .

[48] I. Martinovic, K. Rasmussen, M. Roeschlin, and G. Tsudik, “Authentication Using Pulse-Response Biometrics,” *Commun. ACM*, vol. 60, no. 2, 2017.

[49] D. Coffin, “Two-Factor Authentication,” in *Expert Oracle and Java Security*, Berkeley, CA: Apress, 2011, pp. 177–178.

[50] P. Bours, “Continuous keystroke dynamics: A different perspective towards biometric evaluation,” 2012.

[51] J. Rose, Y. Liu, and A. Awad, “Biometric Authentication Using Mouse and Eye Movement Data,” 2017.

[52] C. Feher, Y. Elovici, R. Moskovitch, L. Rokach, and A. Schclar, “User identity verification via mouse dynamics,” *Inf. Sci. (Ny).*, vol. 201, pp. 19–36, 2012.

[53] “MEKTORY.” [Online]. Available: https://www.ttu.ee/projektid/mektory-est/. [Accessed: 13-Apr-2018].

[54] Tobii Technology AB, “Product Description: Tobii X2-30 Eye Tracker, Tobii X2-60 Eye Tracker.” 2014.

[55] Tobii AB, “Tobii Studio User’s Manual,” *2016*. .

[56] Tobii AB, “Tobii Pro X2-30 screen-based eye tracker.” [Online]. Available: https://www.tobiipro.com/product-listing/tobii-pro-x2-30/. [Accessed: 13-Apr-2018].

[57] Tobii AB, “Tobii Pro Studio eye tracking software, dedicated for UX.” [Online]. Available: https://www.tobiipro.com/product-listing/tobii-pro-studio/. [Accessed: 14-Apr-2018].

[58] “Postimees: Värsked uudised Eestist ja välismaalt.” [Online]. Available: https://www.postimees.ee/. [Accessed: 16-Apr-2018].

[59] “YouTube.” [Online]. Available: https://www.youtube.com/. [Accessed: 16-Apr-2018].

[60] Contributors to the Web Speech API Specification, “Web Speech API Specification,” 2014. [Online]. Available: https://w3c.github.io/speech-api/webspeechapi.html#speechreco-section. [Accessed: 30-Apr-2018].

[61] “SpeechRecognition - Web APIs | MDN.” [Online]. Available: https://developer.mozilla.org/en-US/docs/Web/API/SpeechRecognition. [Accessed: 30-Apr-2018].

[62] D. Walsh, “JavaScript Speech Recognition,” 2016. [Online]. Available: https://davidwalsh.name/speech-recognition. [Accessed: 30-Apr-2018].

[63] “tracking.js.” [Online]. Available: https://trackingjs.com/. [Accessed: 30-Apr-2018].

[64] Kairos AR, “Face Recognition, Emotion Analysis & Demographics.” [Online]. Available: https://www.kairos.com/. [Accessed: 30-Apr-2018].

[65] Kairos AR, “Developing with Kairos · Apiary.” [Online]. Available: https://kairos.docs.apiary.io/#. [Accessed: 02-May-2018].

[66] xLabs Pty Ltd, “xLabs eye, gaze and head tracking via webcam.” [Online]. Available: https://xlabsgaze.com/. [Accessed: 06-May-2018].

[67] xLabs, “xLabs Gaze API Documentation,” 2016. [Online]. Available: http://xlabsgaze.github.io/docs/home.html. [Accessed: 06-May-2018].

[68] Talview, “Frequently Asked Questions - Proview.” [Online]. Available: https://staging.proview.io/faq-main/. [Accessed: 12-Feb-2018].

[69] A. Babu, “Talent bazaar on Talview,” *Bus. Stand. News*, p. 25, Jan. 2015.

[70] Software Secure, “Remote Proctor PRO FAQ - Secure Testing. Anytime. Anywhere.” [Online]. Available: http://www.softwaresecure.com/remote-proctor-pro-faq/. [Accessed: 10-Feb-2018].

[71] Software Secure, “Remote Proctor Pro - Product Data Sheet.” 2008.

[72] “Purchase Remote Proctor Device.” [Online]. Available: https://www.remoteproctoradmin.com/buyrp/. [Accessed: 10-Feb-2018].

[73] “Amazon.com: SecureExam Remote Proctor.” [Online]. Available: https://www.amazon.com/Software-Secure-SRP5702-Rev-1-0/dp/B009XYBPLW. [Accessed: 12-Feb-2018].

[74] L. F. Cochran, L. K. Troboy, and T. L. Cole, “A Test of Integrity: Remote Proctoring In An Online Class,” *J. Bus. Adm. Online*, vol. 9, no. 2, 2010.

[75] Business Wire, “PSI Services LLC Acquires Remote Proctoring Pioneer Software Secure, Inc.,” *Business Wire*, 2017.

[76] “LTI and Moodle - MoodleDocs.” [Online]. Available: https://docs.moodle.org/34/en/LTI_and_Moodle. [Accessed: 12-Feb-2018].

[77] PSI Services LLC, “Clients.” [Online]. Available: https://wwwdemo.psionline.com/en-gb/education/clients/. [Accessed: 12-Feb-2018].

[78] Pearson Education Inc, “Pearson VUE Integrated Platform. Flexible testing options with one streamlined system.” .

[79] Microsoft, “Microsoft Online Proctored (OP) Exam.” [Online]. Available: https://www.microsoft.com/en-us/learning/online-proctored-exams.aspx. [Accessed: 12-Feb-2018].

[80] SA Innove, “Riigieksami vaatlusjuhend.” 2018.

[81] I. Traore and A. A. E. Ahmed, *Continuous authentication using biometrics : data, models, and metrics*. Information Science Reference, 2012.

[82] Riigi Infosüsteemi Amet, “Isikut tõendavate dokumentide päring,” 2012. [Online]. Available: https://www.eesti.ee/est/teenused/kodanik/riik_ja_kodanik/isikukaart. [Accessed: 07-May-2018].

[83] O. M. Parkhi, A. Vedaldi, and A. Zisserman, “Deep Face Recognition,” 2015.

[84] Y. Sun, D. Liang, X. Wang, and X. Tang, “DeepID3: Face Recognition with Very Deep Neural Networks,” Feb. 2015.

[85] F. Schroff, D. Kalenichenko, and J. Philbin, “FaceNet: A unified embedding for face recognition and clustering,” in *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2015, pp. 815–823.

[86] Y. Xu, T. Price, J.-M. Frahm, and F. Monrose, “Virtual U: Defeating Face Liveness Detection by Building Virtual Models from Your Public Photos,” in *Proceedings of the 25th USENIX Security Symposium*, 2016.

[87] N. Erdogmus and S. Marcel, “Spoofing Face Recognition With 3D Masks,” *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 7, pp. 1084–1097, Jul. 2014.

[88] Y. Li, Y. Li, Q. Yan, H. Kong, and R. H. Deng, “Seeing Your Face Is Not Enough: An Inertial Sensor-Based Liveness Detection for Face Authentication,” in *CCS 15: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015, pp. 1558–1569.

[89] K. Niinuma and A. K. Jain, “Continuous user authentication using temporal information,” in *SPIE 7667, Biometric Technology for Human Identification VII*, 2010.

[90] A. Fayyoumi and A. Zarrad, “Novel Solution Based on Face Recognition to Address Identity Theft and Cheating in Online Examination Systems,” *Adv. Internet Things*, vol. 4, pp. 5–12, 2014.

[91] National Science and Technology Council, “Iris Recognition.” .

[92] L. C. F. Araujo, L. H. R. Sucupira, M. G. Lizarraga, L. L. Ling, and J. B. T. Yabu-Uti, “User authentication through typing biometrics features,” *IEEE Trans. Signal Process.*, vol. 53, no. 2, pp. 851–855, Feb. 2005.

[93] S. Mondal and P. Bours, “Person Identification by Keystroke Dynamics Using Pairwise User Coupling,” *IEEE Trans. Inf. Forensics Secur.*, 2017.

[94] J. V. Monaco, N. Bakelman, S.-H. Cha, and C. C. Tappert, “Developing a Keystroke Biometric System for Continual Authentication of Computer Users,” in *2012 European Intelligence and Security Informatics Conference*, 2012, pp. 210–216.

[95] J. Roth, X. Liu, and D. Metaxas, “On continuous user authentication via typing behavior,” *IEEE Trans. Image Process.*, 2014.

[96] H. Saevanee and P. Bhattarakosol, “Authenticating User Using Keystroke Dynamics and Finger Pressure,” in *2009 6th IEEE Consumer Communications and Networking Conference*, 2009, pp. 1–2.

[97] H. Saevanee and P. Bhatarakosol, “User Authentication Using Combination of Behavioral Biometrics over the Touchpad Acting Like Touch Screen of Mobile Device,” in *2008 International Conference on Computer and Electrical Engineering*, 2008, pp. 82–86.

[98] Y. Sun, H. Ceker, and S. Upadhyaya, “Shared keystroke dataset for continuous authentication,” in *8th IEEE International Workshop on Information Forensics and Security, WIFS 2016*, 2017.

[99] S. Mondal and P. Bours, “A study on continuous authentication using a combination of keystroke and mouse biometrics,” *Neurocomputing*, vol. 230, pp. 1–22, Mar. 2017.

[100] S. Mondal and P. Bours, “Continuous Authentication using Mouse Dynamics,” in *International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2013, pp. 1–12.

[101] B. Sayed, I. Traore, I. Woungang, and M. S. Obaidat, “Biometric Authentication Using Mouse Gesture Dynamics,” *IEEE Syst. J.*, vol. 7, no. 2, pp. 262–274, Jun. 2013.

[102] M. Sharif, T. Faiz, and M. Raza, “Time signatures - an implementation of Keystroke and click patterns for practical and secure authentication,” in *2008 Third International Conference on Digital Information Management*, 2008, pp. 559–562.

[103] Biometric Signature ID, “Multi-factor Authentication Using Gesture Biometrics.” [Online]. Available: https://www.biosig-id.com/. [Accessed: 04-Mar-2018].

[104] BioCatch, “Invisible Challenges.” 2017.

[105] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, “Continuous Verification Using Multimodal Biometrics,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 687–700, Apr. 2007.

[106] NIST, “Summary of NIST Standards for Biometric Accuracy, Tamper Resistanse, And Interoperability,” 2002.

[107] X. Liu, L. Kong, Z. Diao, and P. Jia, “Line-scan system for continuous hand authentication,” *Opt. Eng.*, vol. 56, no. 3, 2017.

[108] Fujitsu Global, “Fujitsu PalmSecure.” [Online]. Available: http://www.fujitsu.com/global/solutions/business-technology/security/palmsecure/. [Accessed: 11-Mar-2018].

[109] Fujitsu Frontech North America Inc, “PalmSecure Mouse.” 2016.

[110] A. K. Jain, S. C. Dass, and K. Nandakumar, “Can soft biometric traits assist user recognition?,” in *SPIE 5404, Biometric Technology for Human Identification*, 2004.

[111] K. Niinuma, U. Park, and A. K. Jain, “Soft Biometric Traits for Continuous User Authentication,” *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 4, pp. 771–780, Dec. 2010.

[112] J. R. Pinto, J. S. Cardoso, A. Lourenço, and C. Carreiras, “Towards a continuous biometric system based on ECG signals acquired on the steering wheel,” *Sensors (Switzerland)*, 2017.

[113] S. Vhaduri and C. Poellabauer, “Wearable device user authentication using physiological and behavioral metrics,” in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2017, pp. 1–6.

[114] C. D. Holland and O. V. Komogortsev, “Complex Eye Movement Pattern Biometrics: The Effects of Environment and Stimulus,” *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 12, pp. 2115–2126, Dec. 2013.

[115] R. J. Leigh and D. S. Zee, *The Neurology of Eye Movements*. Oxford University Press, 2015.

[116] Y. Cheung and Q. Peng, “Eye Gaze Tracking With a Web Camera in a Desktop Environment,” *IEEE Trans. Human-Machine Syst.*, vol. 45, no. 4, pp. 419–430, Aug. 2015.

[117] J. San Agustin, H. Skovsgaard, J. P. Hansen, and D. W. Hansen, “Low-cost gaze interaction,” in *Proceedings of the 27th international conference extended abstracts on Human factors in computing systems - CHI EA ’09*, 2009.

[118] H. Skovsgaard, J. S. Agustin, S. A. Johansen, J. P. Hansen, and M. Tall, “Evaluation of a remote webcam-based eye tracker,” in *Proceedings of the 1st Conference on Novel Gaze-Controlled Applications - NGCA ’11*, 2011.

[119] D. C. Niehorster, T. H. W. Cornelissen, K. Holmqvist, I. T. C. Hooge, and R. S. Hessels, “What to expect from your remote eye-tracker when participants are unrestrained,” *Behav. Res. Methods*, vol. 50, no. 1, pp. 213–227, 2018.

[120] D. Bäck, “Neural Network Gaze Tracking using Web Camera,” Linköpings tekniska högskola (Institutionen för medicinsk teknik), 2005.

[121] A. Boehm *et al.*, “SAFE: Secure authentication with Face and Eyes,” in *2013 International Conference on Privacy and Security in Mobile Systems, PRISMS 2013 - co-located with Global Wireless Summit*, 2014.

[122] Bharath S Sirur and Shankar Pendse, “Gaze driven architecture: Adding new dimensions to level of security in computers,” in *2010 3rd International Conference on Computer Science and Information Technology*, 2010, pp. 200–205.

[123] W. Sewell and O. Komogortsev, “Real-Time Eye Gaze Tracking With an Unmodified Commodity Webcam Employing a Neural Network,” in *Proceedings of ACM Conference on Human Factors in Computing Systems (CHI)*, 2010.

[124] Microsoft, “EnumDisplayMonitors function (Windows).” [Online]. Available: https://msdn.microsoft.com/en-us/library/windows/desktop/dd162610(v=vs.85).aspx. [Accessed: 24-Mar-2018].

[125] Microsoft, “EnumDisplayDevices function (Windows).” [Online]. Available: https://msdn.microsoft.com/en-us/library/windows/desktop/dd162609(v=vs.85).aspx. [Accessed: 24-Mar-2018].

[126] “xrandr - ArchWiki.” [Online]. Available: https://wiki.archlinux.org/index.php/xrandr. [Accessed: 24-Mar-2018].

[127] Respondus Inc, “Respondus.” [Online]. Available: https://www.respondus.com/. [Accessed: 11-Mar-2018].

[128] “Safe Exam Browser - About.” [Online]. Available: https://safeexambrowser.org/about_overview_en.html. [Accessed: 11-Mar-2018].

[129] Cyberbit, “Anti-VM and Anti-Sandbox Explained.” [Online]. Available: https://www.cyberbit.com/anti-vm-and-anti-sandbox-explained/. [Accessed: 12-Mar-2018].

[130] “How Malware Detects Virtualized Environment (and its Countermeasures),” 2016. [Online]. Available: http://resources.infosecinstitute.com/how-malware-detects-virtualized-environment-and-its-countermeasures-an-overview/. [Accessed: 12-Mar-2018].

[131] C. Jämthagen, M. Hell, and B. Smeets, “A Technique for Remote Detection of Certain Virtual Machine Monitors,” Springer, Berlin, Heidelberg, 2012, pp. 129–137.

[132] M. Noorafiza, H. Maeda, T. Kinoshita, and R. Uda, “Virtual machine remote detection method using network timestamp in cloud computing,” in *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, 2013, pp. 375–380.

[133] J. Moten, A. Fitterer, E. Brazier, J. Leonard, and A. Brown, “Examining online college cyber cheating methods and prevention measures,” *Electron. J. e-Learning*, 2013.

Lisa 1 – Kommertslahenduste näited

Alljärgnevalt on põhjalikumalt kirjeldatud mõningaid Peatükis 3.2 esitatud laiatarbeliste eksami järelevalve lahendusi.

1 Talview − Remote Proctor/Proview

Talview on Indiast alguse saanud firma, mis on keskendunud nii tööle kui ülikooli kandideerimise protsessi sujuvamaks ja veebipõhisemaks muutmisele [44].

Proview järelevalvesüsteem võimaldab vältida spikerdamist ja kontrollitavaks kehastumist ja lubab kokku hoida testide administreerimiskuludelt [44]. Salvestatakse eksamitegija ekraanil toimuvat ning ümbruses olevat heli ja videot. Süsteem kindlustab, et kandidaat keskendub testi tegemise ajal ekraanile, ruumis on piisavalt valge, taustal pole kahtlasi esemeid ega heli. Sisse logivat kasutajat autenditakse isikut tõendava dokumendi alusel näotuvastusega ning sama funktsionaalsust kasutatakse, kontrollimaks, et kandidaat ei vahetu testi tegemise ajal. Algoritm tuvastab võimalikud eksamikorra rikkumised ja teavitab nendest jooksvalt testi tegijat, võimaldades tollel parandada oma niinimetatud terviklikkuse või aususe skoori (*integrity score*), mis on alustades 100 punkti, aga kahaneb iga rikkumisega [68]. Testi sooritamise jooksul kogutud info edastatakse krüpteeritult põhjaliku logina vaatlejale, Talview firma ise videoid ei näe. Iga tudengi kohta, kelle aususe skoor on alla eelnevalt administraatori poolt määratud piiri, esitatakse foto autentimisprotsessist, taustamüra ja ekraanil toimuva kokkuvõte, suvalisel hetkel tehtud pildid ekraanist ja kandidaadi näost ning video eksamiprotsessist, mida on vaatlejal hiljem võimalik kuni 60-kordse kiirusega järele vaadata, et teha kindlaks, kas protseduurireegleid ka tegelikult eirati. Piisava punktisumma korral antud andmeid vaatlejale ei edastata, mis tähendab ühtlasi privaatsemat kogemust iga ausa testitegija jaoks. Korraga on võimalik ühel ekraanil jälgida kuni 64 kandidaati [69].

Kandidaatidel puudub vajadus eraldiseisvate rakenduste või veebipluginate allalaadimise järele ning eksami sooritamise aeg ja koht ei ole välise vaatleja poolt piiratud, kuigi soovi korral on testi administraatoril võimalik kandidaate reaalajas jälgida. Proview ei piirdu

vaid eksamite ajal tudengite isiku kontrollimisega, vaid võimaldab kogu kursuse vältel kindlaks teha, et ülesandeid lahendab üks ja sama tudeng. Lisaks eksamite vaatlusele ja õppetööle saab seda kasutada ka veebipõhiste intervjuude või muu suhtluse kontrollimiseks.

Miinimumnõuded Proview kasutamiseks hõlmavad vähemalt 640x480 eraldusvõimega veebikaamera, mikrofoni, Chrome või Firefox veebilehitseja olemasolu [68]. Proview toetab operatsioonisüsteeme alates Windows Vistast ja Mac OS X 10.5. Edukaks kasutamiseks peab interneti allalaadimiskiirus olema vähemalt 768 kbit/s ja üleslaadimiskiirus 384 kbit/s ning läbilaskevõime minimaalselt 256 kbit/s, kuigi soovituslik on 512 kbit/s. Vajalik on 1024 MB vaba mälu (RAM). Nõuetele vastavust kontrollitakse eraldi riistvaratesti abil, mille kestus on vähem kui 90 sekundit.

Lisaks täielikult automatiseeritud testimisjärelevalvele pakub firma ka Talview Proctor Engine'il põhinevat täielikku eksamikeskkonda, võimaldades muuseas kontrollida lugemist, kuulamist, kirjutamist, grammatikat, programmeerimisoskust [44]. Talview lahendusi kasutab näiteks Cambridge English Language Assessment [44].

2 Software Secure − Remote Proctor PRO

Software Secure alustas järelevalve pakkumist tark- ja riistvara ühislahendusest, võimaldamaks kontrollida kaugõppe eksamitel toimuvat. Lahenduse põhiobjektiks oli seadeldis Remote Proctor PRO, mis koosnes 360-kraadi kaamerast, mikrofonist ja sõrmejäljelugejast [70].

Esiteks sisenes eksaminand oma õppekeskkonda (näiteks Moodle) [71]. Seejärel tuvastati arvutiga ühendatud Remote Proctor PRO seadme abil kandidaadi isik, võrreldes hetkebiomeetriat kursusega liitumisel registreeritud sõrmejälje ja näopildiga. Kui autentimine ebaõnnestus või seadeldis polnud arvutiga korrektselt ühendatud, keelati eksamil osalemine. Kui kasutaja oli edukalt tuvastatud, käivitus testimisprogramm Securexam, mis võimaldas eksami sooritamise ajal kasutada ainult õppekeskkonda ja blokeeris kogu ülejäänud funktsionaalsuse, kaasa arvatud ligipääsu failidele, internetile ja muudele rakendustele.

Testi tegemise ajal lindistas Remote Proctor PRO seadeldis muutusi ruumis aset leidvas liikumises ja helis. Kogutud andmed saadeti internetiühenduse kaudu Software Secure

serverisse, kust neid vaatasid hiljem veebiliidese vahendusel üle Software Secure palgatud tunnustatud spetsialistid, kelle ülesandeks oli tuvastada eksamikorra rikkumisi, nagu kõrvaliste materjalide või abi kasutamine. Videosalvestis ja ülevaade eksamisooritusest koos potentsiaalsete pettushetkedega edastati asutusele, kes langetas lõpliku otsuse kandidaadi reeglite vastu rikkumise kohta.

Kui eksaminandi internetiühendus katkes eksami sooritamise ajal või polnud piisavalt kvaliteetne videofailide edastamiseks, üritas Remote Proctor PRO tarkvara faile edastada iga kord, kui eksamitegija arvuti uuesti käivitati. Remote Proctor PRO 360-kraadi kaamera ja sõrmejäljelugejaga lisaseadet Software Secure lehel enam ei müüda [72], aga seda on võimalik osta näiteks eBayst või Amazonist [73]. Aastal 2010 oli õpilastele seadme maksumus 200 $ ja järelevalvetarkvara hind 30 $ semestris [74], mistõttu oli tegemist üsna kalli lahendusega. Küll aga saab seadet kasutada korduvalt, st mitme isiku autentimiseks, mistõttu võis pärast kasutust selle edasi müüa või seda ülikoolidelt rentida.

3 PSI − Remote Proctor Now

Alates aastast 2017. kuuluvad Software Secure firma ja nende lahendused PSI Services LLC omandisse [75]. Hetkel kasutusel olev järelevalvelahendus Remote Proctor Now (RPNow) ei kasuta kandidaatide jälgimiseks enam välist seadeldist, vaid kandidaadi internetiühendusega arvutit, veebikaamerat ja mikrofoni, ning on täielikult veebi- ja pilvepõhine. Platvorm on LTI (*Learning Tools Interoperability*) toe olemasolul seotav ükskõik millise õppekeskkonnaga (näiteks Moodle [76]), mis tähendab, et eksamiparoolid, -ajad, tulemused ja muu õppeinfo on automaatselt sünkroniseeritud, vähendades vigade tekke ohtu andmete ümber kandmisel. Tänu sellele võimaldab RPNow hõlpsalt õppekeskkonnas loodud arvutipõhistele eksamitele järelevalvet lisada ja tulemusi hallata.

Õppejõud või eksameid administreeriv isik saab endale harjumuspärases õppekeskkonnas luua eksami ning seejärel RPNow integreeritud keskkonnas seadistada, kui kaua eksam kestab, kas antud eksamile on vaja järelevalvet, millised on eksamil lubatud rakendused, veebilehed ja lisamaterjalid [43].

Eksaminand peab esmalt alla laadima *Flash*'i kasutava RPNow Secure Browser veebilehitseja, mis kontrollib käivitudes veebikaamera, mikrofoni ja piisavalt kiire

internetiühenduse (üleslaadimiskiirusega 125 kbit/s) olemasolu ja et arvutiga ei oleks ühendatud välist ekraani. Sobiva eksami valimisele järgneb kandidaadi autentimine, mille käigus peab tegema foto nii kandidaadist endast kui ka tema isikut tõendavast dokumendist (pass, ID-kaart) ning lindistama video ümbritsevast ruumist, veendumaks, et läheduses pole keelatud materjale või kõrvalisi isikuid. Kui autentimine on edukas, suunatakse eksaminand läbi RPNow veebilehitseja asutuse õppekeskkonda (nt Moodle), kus küsitakse eksami salasõna, mille RPNow sisestab krüpteeritult tudengi nägemata, takistamaks testi sooritamist otse õppekeskkonnas väljaspool RPNow platvormi. Testi tegemise jooksul lindistatakse kandidaadi arvutiekraanil ja ruumis toimuvat nii helis kui videos. Kui kandidaat üritab käivitada rakendust, mille testi administraator on eelnevalt keelanud, takistab RPNow programmi avamist ja kuvab hoiatusakna.

Eksamilindistust kontrollivad pärast testi sooritamise lõppu PSI poolt kvalifitseeritud vaatlejad, kes märgistavad lindistuses esinevad eksimused eksami haldaja (õppejõu, administraatori) poolt määratud eksamikorra vastu, nagu näiteks lubamata materjalide kasutamine, keelatud veebilehtede külastamine või eksaminandi isiku vahetumine. Kui vähemalt kaks vaatlejat on sooritusele hinnangu andnud, kuvatakse eksami haldajale õppekeskkonna PSNow-ga integreeritud lehel soorituste analüüs koos täieliku eksamivideoga, märgistatud rikkumisolukordade ja autentimisinfoga iga tudengi kohta individuaalselt.

PSI lahendusi kasutavad muuhulgas edX MicroMasters, Ivy Tech Community College, Clemson University, Purdue University [77].

4 Pearson VUE

Lisaks ametlikes eksamikeskuses testimisele pakub Pearson VUE ka veebipõhist testimist, ilma et peaks kartma eksamireeglite rikkumist. Pearson VUE lahenduse puhul kasutatakse reaalajas võrgujärelevalvet [78]. Eksami sooritamiseks tuleb eelnevalt registreeruda ja kokku lepitud ajal testi lahendamist alustada. Eksaminande jälgivad veebikaamera ja Pearson VUE Secure Browser veebilehitseja vahendusel Pearson VUE poolt sertifitseeritud vaatlejad, kelle ülesandeks on tuvastada protseduurireeglite rikkumisi [41].

Enne eksami algust luuakse ühendus tervitajaga (*greeter*), kelle ülesandeks on isikut tõendava dokumendi alusel tuvastada kandidaat, korrata üle reeglistik, teha kindlaks veebikaamera ja mikrofoni korrektne töötamine, teostada videokaamera vahendusel põhjalik kontroll testimiskeskkonna nõuetele vastavuse kohta: et ruumis ei viibiks kõrvalisi isikuid, et keskkond oleks piisavalt valgustatud, et keelatud abimaterjale, kaasa arvatud spikrid, lisamonitorid, -arvutid, maalid või postrid seintel, poleks nähtaval või riiete ja juuste vahele peidetud [79]. Kui kandidaat on autenditud ja protokolli vastu eksimisi ei tuvastatud, luuakse ühendus vaatlejaga (*proctor*), kellega saab tehniliste probleemide ilmnemisel vestlusakna kaudu ühendust võtta. Eksam võidakse koheselt kuulutada mittesooritatuks, kui kandidaat lahkub toast, väljub kaadrist või kui ruumi siseneb kõrvalisi isikuid.

Pearson VUE kasutamiseks peab olemas olema veebilehitseja (Internet Explorer 9 või uuem, Microsoft Edge, Chrome, Firefox, Safari), väline või sisseehitatud mikrofon ja veebikaamera eraldusvõimega vähemalt 640x480 [79]. Eksami ajal on lubatud kõrvaklappide kasutamine. Toetatud on operatsioonisüsteemid alates Windows 7 ja Mac OS X 10.8. Lairiba internetiühenduse alla- ja üleslaadimiskiirus peab olema 512 kbit/s, Pearson VUE ise soovitab kaabliühenduse kasutamist. Arvuti ja lisatarvikute tehnilistele nõuetele vastavust on võimalik kontrollida ükskõik millal enne eksami alustamist.

Pearson VUE võimaldab soovi korral eksamit läbi viia ka ilma järelevalveta, võimaldades kandidaadil testi sooritada ajaliselt kellestki teisest sõltumata [78]. Pearson VUE reaalajas vaatlemise lahenduse abil testib kandidaate näiteks Microsoft [79].

Lisa 2 – Kaitsemeetmed

Järgnevalt on esile toodud mõningad kaitsemeetmed, vähendamaks kõrvalise abi kasutamise ja identiteedi jagamise ohtu ehk seda, et kandidaat laseb testi enda isiku alt sooritada kellelgi teisel. Lähtutud on tingimusest, et testimiskeskkonnaks on RangeForce, kus abimaterjalide kasutamine on lubatud.

1 Kontrollitud keskkond

Kõige kindlam viis, veendumaks, et kandidaat teeb eksamit ise ja protseduurireeglitele vastavalt, on nõuda testi sooritamist kontrollitud järelevalvega ruumis, nagu näiteks eksamikeskus, milles kasutatavaid lisaseadmeid, nagu näiteks arvutid, on eelnevalt võimalik seadistada täpselt nii, nagu korraldaja heaks kiidab. Kontrollitud keskkonna puhul saab veenduda, et seintel või laudadel pole keelatud lisamaterjale nagu valemid või spikrid, valgustus on sobiv, eksaminandid istuvad üksteisest piisavalt kaugel ja saavad segamatult töötada.

Kontrollitud keskkonnas on enamasti ka vähemalt üks vaatleja. Riigieksamite puhul on selleks näiteks eksamikomisjon ja Sihtasutus Innove poolt sertifitseeritud välisvaatleja [80], ülikoolide puhul enamasti õppejõud ja nende abilised, kelle ülesandeks on jälgida, et ei eksitaks akadeemiliste tavade vastu keelatud abimaterjale kasutades või kaastudengiga konsulteerides. Osaliselt kontrollitud keskkonda võib tekitada ka virtuaaleksamitel, kasutades selleks näiteks arvutiekraanist ning ruumist 360-kraadi ulatuses videopilti edastavat kaamerat, kuid sellisel juhul ei saa välistada abimaterjalide peitmist laua alla või muu varjava objekti taha ega ka seadmete modifitseerimist kandidaadi poolt.

Teiseks aspektiks on isikutuvastus. Statsionaarõppe puhul tunnevad õpetajad ja õppejõud enamasti oma õpilasi nägupidi, mis takistab kellelgi teisel kandidaadina esinemist. Küll aga ei ole kehastusrünne välistatud eraldiseisvate eksamikeskuste ja selliste kursuste puhul, kus õpe toimub e-keskkonnas, aga eksami tegemiseks peab füüsiliselt kohale tulema. Kehastusründe all võib kannatada ka TTÜ küberkaitse sisseastumistest.

2 Kasutaja pidevtuvastus

Kui kontrollitud keskkonna puhul on raske ette kujutada, et eksaminandid poole eksami pealt vahetuvad, et kellelgi teisel enda eest test ära teha lasta, siis koduses keskkonnas on seda juba märksa keerulisem jälgida. Staatilised süsteemid, kus kasutaja isikut kontrollitakse ainult sisselogimisel, ei ole veebitestide korral piisavalt turvalised ka juhul, kui kasutajat ei kontrollita mitte ainult kasutajanime ja parooli kombinatsiooni, vaid ka biomeetriliste näitajate, nagu sõrmejälg, näotuvastus või silmaiirise skaneerimine, alusel [81].

Üks potentsiaalne meetod kontrollimaks, et testi tegemise vältel kandidaat ei vahetu, on testitegija isiku pidev tuvastamine (ka pidevtuvastus, pidevautentimine, *continuous authentication*). See tähendab, et kasutaja autenditakse sessiooni algul ning sessiooni vältel verifitseeritakse kasutajat pidevalt või perioodiliti [52]. Kasutaja pidevtuvastuse võib jaotada kaheks − aktiivne ja passiivne autentimine [81]. Aktiivse autentimise puhul võidakse kasutajalt teatud ajaperioodi tagant või mõne tegevuse järel nõuda spetsiifilise isikut kinnitava ülesande täitmist, näiteks parooli sisestamine, silmaiirise skaneerimine, teatud fraasi trükkimine või lausumine. Passiivse pidevautentimise puhul kogutakse andmeid taustal ilma kasutaja töövoogu segamata, muutes süsteemi kasutajasõbralikumaks ja eelistatumaks kontekstis, kus kasutaja keskendumine on põhiline.

Variisiku avastamine kasutajat pidevalt tuvastades ei tööta, kui kogu protsessi vältel sooritab tegevusi (registreerumine, sisselogimine, testi lahendamine) keegi teine ja puudub võimalus kontrollida kandidaadi tegelikku isikut, näiteks valitsuse andmebaasis leiduvate dokumentide põhjal. Eestis pakub isiku identiteedi kinnitamiseks ideaalset võimalust ID-kaart, mis on riigipoolseks kinnituseks, et antud isiku nimi ja nägu kuuluvad kokku. Politsei- ja piirivalveametiga andmevahetuslepingu sõlmimisel on võimalik andmebaasist saadud nime ja näo kombinatsiooni võrrelda testitegija omaga ja veenduda, kas isik on see, keda ta väidab end olevat [82]. Kui eksisteerib varasemalt kasutajaga toimunud interaktioon, võib kasutajat tuvastada ka eelneval suhtlusel põhinevate turvaküsimuste alusel.

Kuna kõige raskem on muuta kasutajat ennast iseloomustavaid faktoreid, on järgnevalt analüüsitud mõningaid biomeetrilisi ja käitumuslikke näitajaid, mille alusel võiks RangeForce süsteemi kasutajat testi tegemise ajal korduvalt tuvastada.

2.1 Näotuvastus

Kõige esimesena võiks arvutit kasutava isiku tuvastamiseks tulla pähe visuaalne vaatlus. Näotuvastus põhineb näo tunnusjoonte ruumigeomeetria analüüsimisel [47]. Selle meetodi puhul määratakse, millised on vaadeldavad tunnused, mida erinevate piltide puhul võrrelda, nagu näiteks ninaotsa, suu, silmade vahemaa, ega jälgita kasutaja muid muutuda võivaid tunnuseid, nagu näoilmed, -karvad või juuksed. Üheks oluliseks väljakutseks ja tuvastuse esimeseks sammuks on inimnäo eraldamine ümbritsevast taustapildist ehk näoavastus. Näotuvastus eeldab kasutajalt veebikaamera olemasolu. Õnneks on nüüdisajal paljudel müügil olevatel sülearvutitel veebikaamera juba sisse ehitatud ja ka väliseid veebikaameraid on laialdaselt saadaval.

Näotuvastusel kasutatakse näiteks närvivõrke ja masinõpet [83]. Aastal 2014 saavutas Facebook kombineeritud süva-närvivõrke kasutades DeepFace projekti raames kuulsuste fotosid sisaldaval andmestikul Labeled Faces in the Wild (LFW) tuvastustäpsuse 97.35% [8]. Edasiarendus DeepID3 küündis samal andmestikul lausa 99.53% täpsuseni [84], mis jääb siiski vaevu alla Google FaceNet'i 99.63 protsendist [85]. Võrdluseks, et inimene suudab nägusid tuvastada 97.5% täpsusega [8].

Näotuvastuse edukusel võivad rolli mängida mitmed kasutajast või keskkonnast tulenevad faktorid, nagu näiteks ruumi valgustus, peaasend või näos olevad lisaseadmed. Sobilik süsteem ei tohiks end lasta häirida prille kandvast kasutajast. Adekvaatne näotuvastus nõuab piisavat valgustust.

Näotuvastust kasutades on vaja algsel registreerumisel tehtud fotot, millega edaspidist videovoogu kõrvutada. Baasfoto puhul on oluline, et see pärineks võimalikult usaldusväärsest ja kontrollitavast allikast, sest vastasel juhul võib kandidaat võrdluseks esitada pildi variisikust, kes hiljem tema eest eksamit sooritab. Seega oleks sobiv näiteks kandidaadi riiklik isikut tõendav pildiga dokument, nagu ID-kaart või pass. Puhtalt visuaalsele vaatlusele toetudes ei saa muidugi lõplikult veenduda dokumendi autentsuses ning alati jääb alles kahtlus, et dokument on võltsitud.

Video ei ole tegelikult ei midagi muud, kui seeria järjestatud pilte, mistõttu saab näotuvastust edukalt kasutada ka videovoo puhul. Just video puhul on oluline kontrollida ka näo elavust (*liveliness*), et vältida taasesitusrünnet ehk süsteemi petmist staatilise foto, eellindistatud video, 3D-mudeli [86] või -maski [87] esitamise abil. Virtuaalreaalsustehnoloogia abil on võimalik fotode põhjal koostada ka juhitavat 3D-mudelit kasutaja näost, mida elavuskontrollide petmiseks kasutada [86]. Staatilist fotot saab kontrollida, paludes kasutajal pead liigutada või silmi pilgutada. Video esitamise vältimiseks on võimalik kontrollida kasutaja fookuspunkti, kuvades suvalisse asukohta ekraanil elemendi, mida kasutaja vaatama peab, või paluda kasutajal suvalises järjekorras teatud suunas pead liigutada. Mobiilseadmete puhul saab elavuse kontrolliks lisaks kaamerale kasutada ka güroskoopi ja kiirendusmõõturit [88], kuid arvutite puhul tasub keskenduda fookuspunkti kontrollimisele. Ekstreemsemaks võimaluseks oleks ka kasutaja emotsiooni ja reaktsiooni jälgimine, kuvades näiteks keset töövoogu ekraanile mõne ehmatava pildi või video. Too lahendus loomulikult häiriks kasutaja keskendumist ega ole seetõttu eelistatud. Xu *et al*. on välja pakkunud mitmeid teisigi potentsiaalseid kaitsemeetodeid, nagu pulsist tekkiv perioodiline mikroerisus näotoonis või näo ootamatu valgustamine tava- või infrapunase valgusega, jälgides samal ajal, kas muutub ka esitatava kaadri valgustatus [86].

Kui näotuvastust kombineerida mõne muu ajutise näitaja analüüsimisega, on võimalik kasutajat tuvastada ka siis, kui ta istumisasend (poos) pole optimaalne või ta vaatab veebikaamerast kõrvale. Selleks saab kasutada näiteks riiete värvi jälgimist [89]. Sisse logides salvestatakse kasutaja näo all oleva piirkonna värv, mida hiljem biomeetriliste näitajate puudumisel uuesti kontrollitakse. Kui tuvastatakse kasutaja lahkumine arvutiekraani eest või muutus näojoontes ja/või riiete värvis, on alust arvata, et tegemist pole enam sama kasutajaga.

Traoré *et al.* algoritmi eesmärgiks oli veebikaamera videovoost saadava näopildi järgi tuvastada rikkumisi veebipõhistel eksamitel [11]. Nende pidevautentimissüsteemil õnnestus alati tuvastada variisik. Näotuvastussüsteem lindistas eksamit, tundis ära ja verifitseeris kandidaati näo alusel ning teavitas vaatlejat, kui kandidaat lahkus eksami ajal arvuti eest, testi tegi variisik või testi lahendas mitu tudengit korraga. Probleeme põhjustas muutus testimiskeskkonnas, eriti valgustustingimustes. Näotuvastuse täpsus langes drastiliselt, kui muudeti laualambi asukohta või kustutati valgus.

Fayyoumi ja Zarradi välja pakutud lahendus võrdleb testile registreerumisel andmebaasi salvestatud fotot testi tegemise aegse veebikaamera videovooga [90]. Lisaks sellele tuvastatakse kahesekundiliste videolõikudega, kas kasutaja jälgib ekraani ja on keskendunud eksamiküsimustele vastamisele. Kui leitakse, et kasutaja tähelepanu on mujal ehk võib esineda olukord, kus eksaminand kasutab keelatud abimaterjale, hoiatatakse testitegijat testimiskeskkonna taustavärvi muutusega. Samamoodi teavitatakse kasutajat ka ebaõnnestunud pidevautentimisest. Kui teatud aja jooksul ei õnnestu kasutajat tuvastada, peatab süsteem töö ja palub asendit korrigeerida. Korduval ebaõnnestumisel eeldatakse, et toimub pettus. Võrgukoormuse vähendamiseks kasutab Fayyoumi ja Zarradi lahendus meetodit, kus 30 sekundi tagant tehtud kahe sekundi pikkusest videoklipist valitakse kliendipoolse rakenduse abil välja parima näoilme, eraldusvõime ja valgustustingimusega kaader, mis edastatakse analüüsimiseks serverile.

Video baasil pidevautentimise puhul võib probleemiks osutuda ka kogutud andmete saatmine üle võrgu serveripoolele, kus toimub nende analüüs. Edukaks edastamiseks on vaja piisavalt kiiret internetiühendust, aga ka kasutaja arvuti ressursse (protsessor, mälu). Võrguühendusega seotud probleeme oleks võimalik vähendada, kui algoritm töötaks lokaalses masinas. Edastatavat andmehulka saab vähendada, kui analüüsida videovoogu perioodiliselt ehk võtta vaatluse alla ainult teatud ajahulga möödudes tehtud kaader [11]. Eksami puhul on see lubatud eeldusel, et analüüsitavate kaadrite vahele jääv ajaperiood on piisavalt lühike, et takistada variisikul ilma tabamata arvuti kasutamist.

Isegi, kui eeldada, et sisseastumiseksami kaitsesüsteem teeb edukalt vahet kandidaadi ja variisiku näol, ei ole ainult näotuvastuse rakendamine piisav kaitsemeede. Nimelt oleks sellisel juhul võimalik tekitada olukord, kus veebikaamera on kogu eksami vältel suunatud kandidaadi poole, aga testi lahendab sellest hoolimata keegi teine, kes kaamera vaatevälja ei ulatu. Ohuks on ka juhiste edastamine kandidaadile *bluetooth*-kõrvaklappide kaudu, mis on võimalik, kui ei kontrollita, et kandidaadi kõrvad oleksid katmata.

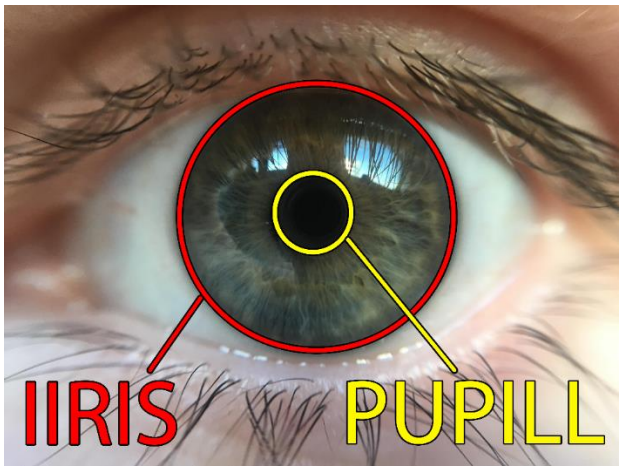
2.2 Hääletuvastus

Üheks autentimismeetodiks on hääletuvastus. Pidevautentimiseks saaks seda kasutada suuliste eksamite puhul, kuid kuna küberkaitse eriala sisseastumiseksam RangeForce keskkonnas ei sisalda suulist osa, ei saa seda antud kontekstis rakendada kandidaadi isiku kontrollimiseks. Seetõttu ei ole käesolevas töös hääletuvastusele keskendutud.

Küll aga on võimalik analüüsida ümbritsevas ruumis olevat heli, et teha kindlaks, et keegi kandidaadile kõrvalt suulisi juhiseid ei edasta. Taustakõne keelamine töötab juhul, kui kandidaadil pole kombeks lahenduskäike iseendaga valjusti läbi arutada. Sisseastumiseksami puhul on vaikusenõue põhjendatud. Taustaheli analüüsist on räägitud käesoleva lisa jaotises 6.

2.3 Iirisetuvastus

Iirisetuvastuseks nimetatakse biomeetrilist isikutuvastust, mis põhineb silma vikerkesta mustril [16]. Iiris on silma värviline osa pupilli vahetus ümbruses (vt Joonis 26), mille värvid võivad inimeseti korduda, kuid struktuur ja mustrid üldjuhul mitte, mistõttu pakub silmaiiris head võimalust kasutajate eristamiseks [91]. Vajalik on kvaliteetse kaamera olemasolu, et määrata küllaltki väikese iirise (diameetriga keskmiselt 11 mm) asukoht võimalikult täpselt. Enamasti kasutatakse selleks silma valgustamist infrapunase või lähi-infrapunase (*NIR − near infrared*) valgusega. Silmaiirise alusel kasutaja tuvastamine on kõige efektiivsem, kui iiris asub kaamerast maksimaalselt ühe meetri (1 m) kaugusel [14].



Joonis 26. Silmaiiris ja pupill (erakogu).

Kuna iirise korrektne tuvastamine nõuab kõrgekvaliteetset või eririistvaralist kaamerat ja kindlat vahemaad sensorist, ei ole see taolisel kujul sobilik kasutaja pidevtuvastamiseks RangeForce sisseastumistesti raames ning käesolevas töös sellele laiemalt ei keskenduta.

2.4 Trükkimise dünaamika

Trükkimise dünaamika[1] on hea meetod kasutaja tuvastamiseks, kuna ei nõua eririistvara, vaid tugineb klaviatuuri kui sisendseadme ja teatud klahvinuhi tarkvara olemasolule. Analüüsida saab nii klahvivajutuse kestust [92], erinevate klahvide vajutamise vahelist aega [93], trükkimisprotsessis esinevaid pause ja trükkimise tempot [94] kui ka seda, kas klahve vajutatakse eraldi või samaaegselt, mille erinevus tuleb esile suurtähti sisaldava fraasi puhul, kus võib kasutada nii Shift- kui CapsLock-klahvi (shift vs caps lock) [92].

Kasutajat saab tuvastada ka trükkimise visuaalsel või helilisel teel [95] või analüüsides klahvidele avaldatud survet [96] [97] − meetodid, mis nõuavad klaviatuurile ja kätele suunatud kaamerat käte asendi ja kuju jälgimiseks, mikrofoni klahvivajutustel tekkiva heli analüüsimiseks või vajutustugevuse kohta informatsiooni koguvat survetundlikku klaviatuuri. Võttes arvesse eeldust, et kasutajal on vaid üks veebikaamera, mis võib sülearvutite puhul olla integreeritud ja seega raskesti klaviatuurile suunatav, ja soovi kasutada ainult olemasolevat lihtsasti kätte saadavat riistvara, on surve, käte asendi ja trükkimise visuaalne analüüs antud töös kõrvale jäetud.

Kuna klahvivajutuste dünaamika puhul on tegemist käitumusliku biomeetriaga, on ründajal või variisikul seda äärmiselt raske imiteerida ka originaalkasutaja tegevuse vaatlemise tagajärjel [95]. Lisaks võib ajapikku kasutaja trükkimisstiilis esineda muutusi, mis on tingitud näiteks käte väsimisest pikaaegse kirjutamise tagajärel või oskuste arenemisest [90] ja mis mõjutavad tuvastusprotsessi efektiivsust. Trükkimine võib samuti sõltuda klaviatuurist ja selle harjumuspärasusest kasutajale [98].

Trükkimisstiili saab kontrollida staatiliselt, näiteks parooli sisestamisel sisse logimise ajal. Eeldusel, et see protsess on varem korduvalt toimunud, on võimalik lisaks parooli korrektsusele käesoleva sisestuse trükkimisdünaamika andmeid võrrelda varasematega, et teha kindlaks, kas parooli sisestas sama isik, mis varem. Selline lahendus takistab kõrvalistel isikutel kontole ligi pääseda juhul, kui kasutaja parool ise on teada. Küll aga ei takista see kõrvaliste isikute ligipääsu juba alanud seansi korral [99]. Lisaks staatilisele tuvastusele on võimalik klahvivajutuste põhjal kasutajat autentida pidevalt [93] ja perioodiliselt [94], analüüsides trükkimist teatud hulga tähemärkide sisestamise või pausi

[1] Antud töös on sünonüümidena käsitletud termineid trükkimise dünaamika, klahvivajutuste dünaamika, trükkimisstiil.

esinemise järgselt. Pidevtuvastuse puhul on oluline, et vale kasutaja tuvastataks nii kiiresti kui võimalik ehk väheste klahvivajutuste järel [50] ja et õiget kasutajat ei eemaldataks süsteemist esimese kõrvalekalde peale, vaid alles siis, kui usalduskvoot on langenud alla teatud piiri [50]. Trükkimisstiili jälgimine on passiivne autentimisviis, kuna seda saab teostada ilma kasutajalt eraldi keskendumist nõudmata, ja protsess ei sega üldjuhul kasutaja tööjärge [94].

Mondal ja Bours olid ühed esimestest, kes analüüsisid ka ühe käega trükkimise tagajärjel tekkinud andmestikku ning kinnitasid püstitatud hüpoteesi, et ühe käega trükkimise tuvastuse edukus erineb suuresti mõlema käega trükkimise omast [93]. Seetõttu peaks süsteem arvesse võtma ka hetki, kus kasutaja sisestab teksti ajutiselt ainult ühe käega, ning ei tohiks kasutajat koheselt süsteemist välja visata.

Kuna RangeForce testid eeldavad käskude trükkimist virtuaalmasina terminalis, sobib kasutaja klahvivajutuste dünaamika analüüsimine eksaminandi identiteedi kontrollimiseks. Soovides suurendada analüüsitava trükiteksti hulka, võib kandidaadil paluda enne eksami algust ümber trükkida ette antud tekst näiteks akadeemilisest korrast kinni pidamise kohta või keelata testi sooritamise ajaks kopeerimise ja kleepimise operatsioonid [98], mis tähendab, et isegi, kui eksaminand leiab veebist sobiva käsu, peab ta selle käsitsi ümber kirjutama, suurendades analüüsitavate klahvivajutuste andmestikku, mis omakoda võimaldab kasutajat täpsemini tuvastada. Võrdlusandmestiku genereerimiseks ja kaitsesüsteemi treenimiseks võib süsteemi sisse logides paluda sisestada enamlevinuid terminalikäske, mis ka ülesannete lahendustes esinevad.

Klahvivajutuste kogumisel on oluline andmestiku privaatsuse tagamine, kuna kogutud andmed võivad sisaldada kasutajanimesid ja paroole või tundlikku infot kasutaja enda kohta [98]. Tundlikud andmed tuleks enne trükkimisinfo salvestamist sellest kindlasti eemaldada või loobuda andmestiku salvestamisest. Kuna RangeForce testi puhul on kirjutamisstiili analüüsimine oluline vaid sessiooni vältel, tuvastamaks kasutaja vahetumist, ega vaja loodetavasti hilisemat uurimist, puudub vajadus andmete salvestamiseks. Lisaks ei nõua RangeForce ülesanded kasutajalt oma personaalsete andmete avaldamist, mistõttu ei saa sisestatud teksti nimetada tundlikuid andmeid sisaldavaks.

Seega võiks sobilik stsenaarium olla analoogne Roth *et al.* pakutuga [95], kus süsteem käivitub parooli sisestades ja salvestab sellest momendist alates 30 sekundi jooksul kasutaja klaviatuuri kasutust, mis muutub edaspidise võrdluse baasiks. Kui kasutaja lahkub arvuti tagant, lõppeb sessioon ja biomeetriline võrdlusbaas kustutatakse. Mõistlik on analüüsida kahe või enama klahvivajutuse kombinatsioone, näiteks kuidas erineb ’chown’ ja ’touch’ käske sisestades klahvivajutuste ’c’ ja ’h’ kestus ja vajutuste vahel olev aeg.

Küll aga ei piisa ainult trükkimisprotsessi jälgimisest, sest see lubaks konsulteerida mõne teise ruumis viibiva isikuga, sisestamaks terminali nende ette öeldud käske. Samuti ei ole variisiku tuvastamine ainult trükkimise baasil kohene [95], kuna nõuab võrreldava andmestiku kogumist.

2.5 Hiire kasutusviis

Teiseks laialdaselt levinud sisendseadmeks on arvutihiir ja puutepadi (*touch pad*). Hiire puhul saab jälgida näiteks kursori asukohta ekraanil, hiire liigutamise suunda, kiirust, kiirendust ja sujuvust, liikumisvahemaad ja pausi tegevuste vahel [100], nuppude vajutamist ning lahti laskmist ja rulliku (*mouse wheel*) kasutamist [99]. Klikkimisel saab eristada üksikvajutust, topelt-klikki ja lohistamist. Eririistvaralise puutepadja puhul on võimalik analüüsida ka vajutuse survetugevust. Käesoleva töö autoril on näiteks komme oma hiirt aeg-ajalt hetkeks kergitada ja seejärel samasse kohta tagasi asetada, mis põhjustab kursori koha peal jõnksutamist ja võib seetõttu olla üheks kasutajale iseloomulikuks jooneks.

Ka hiiredünaamika jälgimisel on vajalik õppeperiood, et tuvastada konkreetsele kasutajale iseloomulik hiirekasutus. Tegelikult on hiire abil kasutajat lihtsam tuvastada pidevautentimisel kui staatilisel autentimisel [101], kus kogutavaid andmeid on kordades vähem. Sharif *et al.* [102] implementeerisid andmestiku kogumise klahvivajutuste analüüsimise ja värviakna abil, kus kasutaja pidi kindlas järjekorras neljal värviruudul klikkima. Sayed *et al.* [101] on selle probleemi lahendamiseks välja pakkunud sisselogimissüsteemi, kus kasutaja tuvastatakse joonistatava sümboli järgi. Nii võib hiirekasutust võrrelda ka allkirjaga, mis peaks igal kasutajal olema unikaalne. Taolist alternatiivi traditsioonilisele salasõnaga sisselogimisele pakub näiteks BioMetric Signature ID [103].

Rose *et al.* leidsid, et vertikaal- ja horisontaalsuunas liigutatakse hiirt tavaliselt sirgjooneliselt, samas kui diagonaalidel tekib pigem kaarjas joon, kusjuures kaardumise kraad ja suund on iga kasutaja puhul unikaalne, pakkudes seega võimalust isiku tuvastamiseks [51].

BioCatch suurendab hiire kasutusviisi jälgimist erinevate kasutaja jaoks märkamatute kõrvalekalletega, nagu näiteks hetkeks hiire ekraanilt peitmine või kursori sihtpunktist kergelt kõrvale kallutamine, sundides nii kasutajat aktiivselt hiirt liigutama, et seda jälle ekraanilt leida, või oma liigutust korrigeerima [104]. Esimese meede on efektiivne kasutajatuvastusel ja teine välistab olukorra, kus tegevusi sooritab arvuti, mitte inimene.

Dünaamika jälgimisel võib takistusi osutada hiire tüüp. Mehaanilise hiire puhul, mis ei ole küll enam nii levinud, võib funktsionaalsust mõjutada liikuvate osade vahele takerduv lint, optilisel hiirel valgust peegeldav või läbipaistev aluspind. Mõne hiire puhul tekib raskusi kiirete liigutuste salvestamisega [52]. Sõltuvalt oma füüsilisest asukohast (kodu, kool, ühistransport) võib sülearvuti kasutaja sisendseadmena kasutada kas välist hiirt või arvutile sisse ehitatud lahendusi, nagu osutushoob (näpuhiir ehk *pointing stick*) või puutepadi (*touch pad*), millest sõltuvalt kasutusviis erineb ja valmistab raskusi kasutaja profiili koostamisel. Küll aga võib eeldada, et sisseastumiseksami lahendamise ajal kasutaja oma sisendseadet liiga sageli ei muuda. Erandiks võivad olla vaid sülearvuti omanikud, kelle puhul esineb olukord, kus intensiivse trükkimisprotsessi ajal eelistatakse kiireks hiireliigutuseks pigem puutepatja või osutushooba kui sülearvuti kõrval asuvat arvutihiirt.

Hiiredünaamikat tasub pidevautentimise täpsuskindluse tõstmiseks kombineerida klahvivajutuste dünaamikaga või silmade fookuspunkti analüüsimisega (vt Lisa 2 jaotised 2.4 ja 3).

2.6 Hiire kaasabil autentimine

Hiire abil autentimine ei pea tähendama vaid kasutaja hiireliigutuste jälgimist. Kuna arvutihiire sisse on võimalik integreerida mitmeid autentimistehnoloogilisi lisalahendusi, saab hiirt kasutades jälgida kasutaja käelt kogutavaid andmeid. Sim *et al.* on kasutaja pidevtuvastamiseks välja pakkunud idee kasutada sõrmejäljelugejaga hiirt [105]. Koos näotuvastusega pakub see kaitset, kui kasutaja sirvib veebilehti või e-posti, kasutades kerimiseks hiirt, kuid kuna trükkimise ajal on käed klaviatuuril ja peaasend võib olla alla

suunatud, ei ole tol hetkel võimalik kasutajat edukalt tuvastada. Lisaks on tänapäeval sõrmejälge arvestatavalt lihtne võltsida kasvõi skänneri ja 3D-printeri abil. Teisalt, USA valitsusorganisatsiooni National Institute of Standards and Technology sõnul ei ole kahelt protsendilt inimkonnalt kvaliteetset sõrmejälge üldse võimalik võtta [106]. Seetõttu ei ole ainult hiirel asuva sõrmejäljelugeja ja näotuvastuse abil kasutaja autentimine praktiline.

Liu *et al.* [107] on uurinud kasutaja pidevtuvastamist käekuju ja -joonte kaudu juhtseadmele paigutatud sensorite abil. Nemad keskendusid juhtkangidele (*operating rod*), nagu on lennukil, mootorrattal või ekskavaatoril, aga tegelikult saab sama tehnoloogia üle kanda ka arvutihiirtele.

Midagi analoogset on teinud Fujitsu oma PalmSecure [108] tehnoloogiat toetava hiirega [109]. Peopesas asuvate veenide järgi autentimist peetakse hetkel kõige turvalisemaks biomeetriliseks tuvastusmeetodiks, sest veenide asetus on igal inimesel unikaalne, ei muutu elu jooksul ning ei sõltu välisteguritest, nagu temperatuur või niiskus. Infrapunase valguse abil veenivere hapnikusisalduse jälgimine raskendab suuresti antud biomeetrilise näitaja võltsimist. Kahjuks on käesoleval hetkel Fujitsu PalmSecure tehnoloogia puutevaba, mis tähendab, et kuigi veenimustri lugeja on spetsiaalse arvutihiire sisse integreeritud, on kasutaja tuvastamiseks tarvilik peopesa hiirelt tõsta ja kätt seadme kohal hoida. Seetõttu ei ole tegemist täielikult passiivse ja pideva autentimismeetodiga.

Eelpool mainitud lahendused eeldavad spetsiaalse riistvaraga hiire olemasolu, mida ei saa sisseastumiseksami sooritajalt nõuda, mistõttu ei ole need antud kontekstis rakendatavad.

2.7 Kergbiomeetria

Kergbiomeetriaks (*soft biometrics*) nimetatakse inimkeha eristatavatel välistunnustel (sugu, vanus, kasv, kaal, rass, nahavärv, silmavärv, juustevärv, armid, sünnimärgid, tätoveeringud) põhinevat liigituslikku, kuid enamasti mitte individualiseerivat biomeetriat [16]. Kuigi need tunnused pole unikaalsed ja neid on võimalik muuta ning võltsida (meik, kontsad, mask, parukas), annavad nad siiski kasutajast mõningase ülevaate, mistõttu saab neid kasutada koos teiste autentimissüsteemidega [110]. Kergbiomeetrilisi tunnuseid ei hoita andmebaasis, vaid need salvestatakse käesoleva sessiooni võrdluse tarbeks sisselogimise hetkel [111].

RangeForce puhul tasuks kaaluda näiteks soo, rassi, naha- ja juustevärvi ning näopiirkonnas olevate armide, sünnimärkide ja tätoveeringude jälgimist, kuna nende kohta on võimalik infot koguda veebikaamera vahendusel ja need kergbiomeetria tunnused toetaksid isiku kontrollimist näotuvastuse baasil.

2.8 Muu

Kasutajat saab pidevtuvastada ka näiteks ajutegevuse alusel, jälgides pea külge kinnitatud anduritega ajusignaale või muutusi hemoglobiinis (veres) näiteks spektroskoopia või elektroentsefalograafia (EEG) abil [5]. Ajutegevus sõltub keskkonnast, ajutisest ja füüsilisest seisundist, kuid võrreldes ajutegevust puhkehetkel ja ülesande lahendamise (trükkimise) ajal võib inimeste lõikes näha mõningaid erinevusi, mille alusel kasutajaid tuvastada, kusjuures paremini ilmnevad need just puhkehetkel. Ajuaktiivsust jälgides on võimalik kontrollida, kas sensoreid kandev kandidaat tegeleb parasjagu sisseastumiseksami lahendamise või millegi muuga.

Ka elektrokardiogrammiga (EKG) südametegevust mõõtes on võimalik kasutajat autentida [3]. Küll aga võib südametegevuse abil kasutaja tuvastamine olla ajamahukam protsess, sest kui näiteks näopildi puhul on analüüsimiseks võimalik saada 30 kaadrit sekundis, siis süda lööb keskmiselt 1−1.5 korda sekundis, mistõttu kulub süsteemi treenimiseks kauem aega. Probleemiks võib osutuda ka füsioloogiliste ja psühholoogiliste muutuste, nagu kehaline aktiivsus, toitumine, haigused, hingamine või elektroodide asetus, mõju EKG signaalidele, mida tuleb sobivat robustset autentimissüsteemi disainides arvesse võtta. Südametegevuse mõõtmist autorooli integreeritud elektroodidega on kasutatud ka autojuhtide fookuse ja väsimustaseme kontrollimiseks ning nende pidevaks isikutuvastuseks [112].

Iga inimkeha reageerib erinevalt, kui seda mõjutada madalpinge impulsiga, sest elektrijuhtivus ja signaali nõrgenemise intensiivsus sõltub luustruktuurist, lihaste tihedusest, rasvasisaldusest ja veresoonte asendist ning suurusest [48]. Seetõttu saab kasutajat tuvastada, kui suunata ühte peopessa madalpinge elektriimpulss ja ülekande tulemust teisest peopesast mõõta. Kui teiste autentimismeetodite (näotuvastus, sõrmejälg) korral on süsteemide petmine taasesituse meetodil lihtne, siis keha reaktsiooni elektrilisele impulsile on äärmiselt raske replikeerida Taasesitamiseks on vaja täpselt sama juhtivusega riistvara, mistõttu on tegemist ühe turvalisema tuvastusmeetodiga. Elektrit juhtivast materjalist või elektrit juhtiva kihiga kaetud klaviatuuri (ja hiire)

olemasolul saab trükkimise ajal sõrmeotstel edastatud ja mõõdetud elektriimpulsse kasutada kasutaja pidevtuvastamise eesmärgil.

Ka nutikellade ja aktiivsusmonitoride sensoritest kogutud info (sammude arv, südamerütm/pulss, kalorikulu) abil on võimalik kasutajat tuvastada [113], kuigi antud meetodi puhul on kasutaja edukaks tuvastamiseks vaja laialdast võrdlusandmestikku kasutaja tegevuse ja kehalise aktiivsuse kohta. Küll aga saaks aktiivsusmonitore kasutada, kontrollimaks kasutaja reaktsiooni erinevatele stiimulitele, näiteks südamerütmi löögisageduse suurenemine äkilise ehmatava foto või videoklipi kuvamisel ekraanile.

Kõik antud peatükis mainitud tuvastusmeetodid on kasutaja jaoks passiivsed, see tähendab, et kasutaja tööjärge ei segata, vaid autentimine toimub taustal. Küll aga nõuavad käsitletud tuvastusmeetodid eririistvara või lisaseadmete olemasolu, mistõttu ei ole ükski käsitletud meetod TTÜ küberkaitse sisseastumiseksami jaoks sobilik.

3 Silmade liikumise ja fookuspunkti jälgimine

Silmade liikumine kuulub käitumusliku biomeetria alla. Silmaliikumisdünaamika puhul jälgitakse pilgu liikumist ekraanil. Sageli on selle professionaalselt tegemiseks vaja eririistvara, nagu peatugi [114], infrapunase filtriga kaamera ja infrapunase valguse allikas, et suurendada pupilli avastamise ja jälgimise täpsust, aga mõne lihtsama lahenduse puhul piisab ka sisseehitatud veebikaamerast. Silmade liikumine sõltub nii nende füüsilisest ehitusest kui ka neuroloogilistest faktoritest [115], mistõttu on masina abil inimsilma tegevuse imiteerimine keeruline [114]. Silmade liikumise dünaamika jälgimist kasutatakse muuhulgas kasutajaliideste ja reklaamide analüüsimiseks, silmahaiguste diagnoosimiseks [116] või sisendseadme asemel nende erivajadustega inimeste puhul, kes ei saa arvutit tavapärasel moel hiire ja klaviatuuri abil kasutada [117].

Probleemiks on peaasendi muutumine jälgimisprotsessi ajal [118], [119]. Kasutaja silmade või pea külge kinnitatavad süsteemid töötavad paremini kui arvuti küljes oleva kaameraga süsteem, mis ei võta arvesse kasutaja pea liikumist ekraani suhtes ja töötab hästi vaid seni, kuni peaasend on sama, mis kalibreerimise ajal. Üheks võimalikuks lahenduseks oleks kaasata näotuvastusmeetmeid ning näoasendi ja silmade positsiooni abil näos pilgu liikumise jälgimist parendada. Taolise lahenduse näotuvastuseks ja pilgu jälgimiseks on välja pakkunud näiteks Bäck [120] ning Cheung ja Peng [116]. Bäck võttis

pea asendit arvesse silmaiirise, silma välisnurga ja ninasõõrmete abil. Antud tunnusjooned valiti, kuna neid on ülejäänud näost lihtne avastada ja need ei sõltu kasutaja emotsioonidest. Bäcki süsteem ei töötanud küll sama hästi, kui tol hetkel turul olevad, aga pakub siiski alternatiivi infrapunast valgust kasutavatele lahendustele. Cheung'i ja Peng'i veebikaameraga arvutile mõeldud meetodiga eraldati samuti näokujutisest silmaala, millest omakorda tuvastati iirise keskme ja silma sisenurga (silmatorkavam ja vähem tundlik näoilme muutumisele kui välisnurk) asukoht, mille alusel pilgu suunda arvutada. Erinevate valgustingimuste (päevavalgus, LED-, luminofoorlamp) ühtlustamiseks ja näopiirkonna eraldamise hõlbustamiseks reguleeriti valgustusest tulenevaid heledustasemeid. Pea asendi kalkuleerimiseks jälgiti mitmeid punkte põskedel, kulmudel, silmadel, ninal ja suul. Cheung'i ja Peng'i välja pakutud lahendus suudab pilku jälgida ilma eelneva treenimiseta. Vähese peaasendi muutuse (kuni 15 kraadi) ja staatilise näoilme korral saavutati ligikaudu 2.27-kraadine täpsus.

Pilgujälgimislahendusi mõjutab näiteks silmade kaadrist väljumine ja peaasendi muutumine [119]. Infrapunalahendusi kasutades võib takistavaks faktoriks osutuda ka prillide kandmine, sest klaasid võivad peegeldada arvutiekraanilt tulevat valgust ja takistada seega silma tuvastamist. Tavavalgusega pole prillid niivõrd suureks takistuseks [116]. Kindlasti nõuavad pilgujälgimisrakendused eelnevat kalibreerimist, et kasutaja pilgu suunda korrektselt jälgida.

Silmade fookust isikutuvastuse eesmärgil on uuritud näotuvastust ja pilku ühendava SAFE autentimissüsteemi raames [121], kus kasutaja valib registreerumisel salajaste ikoonide kogu, millest üht suvalist hilisemal sisse logimisel sarnaste peibutusikoonide seast tuvastama ja silmadega jälgima peab. SAFE lahendus kasutab seadme (arvuti, telefon) esikaamerat, kaht infrapunase valguse allikat ja üht infrapunafiltriga kaamerat, mille abil tuvastatakse kasutaja pupillide asend ja liikumine.

Sirur ja Pendse on välja pakkunud hääle, silmade ja pilgutamise kombinatsiooniga arvuti kontrollimise lahenduse [122], kus kasutaja kannab spetsiaalset kiivrit, mille külge on kinnitatud kaks kaamerat, filtrid ja infrapunase valguse allikas. Kuna silmaiiris ja pupill neelavad infrapunast valgust erinevalt, on võimalik paika panna pupilli asukoht ja vaate suund. Kaameratest saadava info põhjal arvutatakse välja kasutaja silmade vaatenurk ekraani suhtes ja kasutajale omased iirist kirjeldavad atribuudid, mille alusel on võimalik

isikut tuvastada. Sirur'i ja Pendse lahendus erineb eelnevatest selle poolest, et võtab enam arvesse ka asiaatide silmade ehitust ja silmamuna osaliselt katvat silmalaugu.

Eririistvarata on pilgujälgimist uurinud Sewell ja Komogortsev [123], kes kasutasid oma töös sülearvuti sisseehitatud kaamerat, koolile või kontorile sarnanevaid valgustingimusi ja närvivõrku, mis treeniti pupilli liikumist jälgima.

Eeldatavasti sõltub silmade liikumise dünaamika täidetavast ülesandest. Ajalehe veebilehte uurides liiguvad silmad teistmoodi kui RangeForce süsteemis küberkaitse sisseastumiseksamit lahendades (vt Peatükk 5.5.3). Seetõttu on see hea meetod kindlustamaks, et kaamera ees olev isik tegeleb aktiivselt eksami lahendamisega, mitte ei lase variisikul eksamit enda eest sooritada, olles ise mõnel muul veebilehel, kaamera näotuvastuse petmiseks enda poole suunatud.

Antud kaitsemeedet oleks võimalik üle kavaldada, kasutades eksami lahendamiseks kaht ekraani, kus mõlemal kuvatakse sama pilt RangeForce testist, kusjuures kaamera on suunatud tegeliku kandidaadi, mitte variisiku, poole. Nii vastab tegeliku kandidaadi silmade liikumine testimiskeskkonna kasutamisel eeldatavale. Et sellist situatsiooni välistada, tuleb arvesse võtta, et silmade liikumine on korrelatsioonis hiire liikumisega (vt Peatükk 5.5.2). Kuna enamasti fikseeritakse esmalt silmadega arvutiekraanil fookuspunkt, kuhu seejärel hiirega liigutakse, mitte vastupidi, siis võib eeldada, et ilma valjusti oma kavatsustest tegelikule kandidaadile teada andmata ei saa variisik hiirt soovitud kohta liigutada nii, et tegeliku kandidaadi silmad keskenduksid kursori asemel ekraaniobjektile, millel lõpuks peatutakse. Omavahelist suulist ja kirjalikku kommunikatsiooni saab takistada ruumiheli analüüsides, märkides ohukohtadena inimkõne kostumise või trükkimisheli esinemise ajal, kui RangeForce süsteemis tekstisisestust ei toimu.

4 Välise lisaekraani keelamine

Mõned võimalikud ründestsenaariumid kasutavad ära võimalust duplitseerida pilti mitmel monitoril. Näiteks võib silmade liikumist ja näotuvastust kasutavat kaitsesüsteemi petta, kui arvutis sooritab eksamit variisik, kuid näotuvastust teostav ja silmade liikumist analüüsiv kaamera on suunatud variisiku sooritust lisaekraanilt jälgiva tegeliku kandidaadi suunas. Nii liiguvad kandidaadi silmad RangeForce süsteemiga kooskõlas

ning on keerulisem tuvastada, et tegelikult kandidaat vaid jälgib ekraanil toimuvat. Sellest tulenevalt on oluline teha kindlaks lisaekraani olemasolu ning paluda kasutajal see eemaldada või takistada süsteemi käivitumist. Näiteks Windowsi operatsioonisüsteemi puhul on selleks võimalik kasutada funktsiooni EnumDisplayMonitors [124] või EnumDisplayDevices [125] ja Linuxil tööriista xrandr [126].

5 Väliste rakenduste keelamine

Selleks, et eksaminand ei saaks testi sooritamise ajal suhtlusprogrammide kaudu abilistega konsulteerida, tuleks keelata välised rakendused nii kasutaja arvutis kui ka RangeForce virtuaalmasinas. Üks võimalus selleks oleks kasutada olemasolevaid ekraanilukustusprogramme, mis takistavad rakenduste vahelist navigeerimist testi tegemise ajal. Alternatiivselt võib disainida spetsiaalselt RangeForce sisseastumiseksami tarbeks koostatud turvalise veebilehitseja, milles on võimalik avada vaid sisseastumiseksami keskkond ja mis teavitab ülikooli, kui veebilehitseja aken pole aktiivne ehk on alust arvata, et kasutajal on tol hetkel lahti mõni teine programm. Turvalisest veebilehitsejast väljumise takistamiseks võib keelata hiire paremkliki, funktsiooniklahvid või muud akende vahel liikumist võimaldavad klahvikombinatsioonid (Ctrl+Alt+Del, Alt+Tab). Turul on mitmeid analoogseid kommertslahendusi, näiteks Respondus [127] või Safe Exam Browser [128], kuid kaaluda võib ka spetsiaalset CD-lt käivituvat lukustussüsteemi [38]. Teine variant on tarkvaraliselt muude programmide avamine lubada, kuid pidada arvestust aktiivsete akende üle ja kui neid tuvastatakse lubatud limiidist rohkem, salvestada hilisema ülevaatamise eesmärgil kuvapilt kasutaja ekraanist ning kuvada hoiatus, mis palub aken sulgeda.

Kuna RangeForce test toimub virtuaalmasinas, tuleb otsustada, milliseid rakendusi ja veebilehti ning millisel määral blokeerida lokaalses masinas ja milliseid virtuaalmasinas, kui üldse. Koostöös RangeForce keskkonna arendajatega oleks mõeldav süsteemisiseselt sisseastumiseksami tarbeks ainult teatud rakenduste ja veebilehtede lubamine. Eksaminandidel on lubatud kasutada otsingumootoreid (Google, Bing), kuid keelatud vahetada infot suhtlusprogrammide (Facebook, VK) vahendusel. Seega peaks vähemalt ühes skoobis olema lubatud veebilehitseja kasutamine, aga piirangutega, nii et keelatud leheküljed oleksid blokeeritud. Tõenäoliselt oleks kõige lihtsam keelata kõik rakendused lokaalses masinas ja lubada osaliselt virtuaalmasinas, kus kontrollimine ja tuvastus on

lihtsam. Samas on võimalik hiljem logifailidest saada infot testi jooksul avatud rakendustest ja sooritatud tegevustest, mispuhul ei oleks tarvilik virtuaalmasinas ühtegi rakendust blokeerida, eeldusel, et kandidaati on enne testi tegemist keelatud rakendustest teavitatud. Igatahes vähendab kontrolli laiendamine RangeForce keskkonda kõrvaliste rakenduste kasutamise ohtu.

Lukustusbrauserit saaks petta, kui lokaalses masinas jooksutada virtuaalmasinat, milles omakorda käivitada lukustusbrauser, milles avaneb RangeForce test. Nii oleksid rakendused blokeeritud vaid kasutaja lokaalses masinas jooksvas virtuaalmasinas, mitte lokaalses masinas endas, võimaldades lokaalses masinas blokeeringust hoolimata kõrvalisi programme kasutada. Et selline olukord välistada, on vaja tuvastada, kas lukustusbrauser töötab virtuaalkeskkonnas või mitte. Selleks võib näiteks kontrollida/uurida hüperviisori olemasolu CPUID järgi [129], registrivõtmeid, mälu, virtuaalmasina ja hosti vahelist suhtluskanalit, protsesse ja faile, MAC-aadressi, BIOS-i seerianumbrit [130], väljuvate IP-pakettide TCP-päiste kontroll-lippe, eluiga, ID-sid [131] ja ajatempleid [132]. RangeForce testi lahendamiseks mõeldud lukustusbrauser ei tohi käivituda virtuaalmasinas. Selle asemel tuleb kasutajat tekkinud olukorrast teavitada, paluda virtuaalmasinat mitte kasutada ning brauser sulgeda.

Sellised ennetusmeetmed välistaksid ekraanijagamis- ja suhtlusprogrammide kasutamise nii lokaalses kui ka virtuaalmasinas. Alternatiiviks väliste rakenduste keelamisele võiks olla ka pidev või perioodiline kuvapildi jälgimine, tuvastamaks keelatud rakendusi, kuid lukustusbrauseri kasutamisel muutub kuvapildi eraldi jälgimine tarbetuks, mistõttu ei ole seda kaitsemeedet antud töös lähemalt käsitletud.

Kui testitegemise keskkond on isoleeritud, tuleb aga kaaluda varianti, et eksaminand kasutab info edastamiseks ja juhiste saamiseks lisaseadmeid, nagu ruumis viibiv kõrvaline isik, teine arvuti või nutitelefon, mistõttu on oluline jälgida ruumi heli ja videopilti.

6 Ruumi helianalüüs

Kui arvutipõhine suhtlus erinevate ekraanijagamis- ja suhtlusprogrammide abil on keelatud, tuleks kontrollida ka seda, et infoedastus ei toimuks suuliselt või muude lisaseadmetega. Selleks oleks praktiline kuulata ruumi taustaheli ning tuvastada sealt

inimkõne. Kuna sisseastumiseksami puhul on võimalik nõuda täielikku vaikust, välistades ka kandidaadi valjuhäälse arutelu, viitab taustal esinev kõne kõrvaliste isikute viibimisele ruumis.

Kõnetuvastust võivad häirida muud ruumis esinevad helid, nagu tooli liikumine, klahvivajutuste heli, hingamine, köhimine. Selleks, et iga vähimgi heli kõnetuvastussüsteemi ei käivitaks, võib analüüsida heli valjust, sagedust või kestust ja süsteemi eelnevalt positiivsete (kõne, sosistamine) ja negatiivsete (hingamine, köhimine, konditsioneer, linnaliiklus) näidistega treenida [33]. Et välistada taustaheli analüüsimise saboteerimist mikrofoni blokeerimise või muu analoogse meetodi näol, võib ebaregulaarse perioodi järel kõlaritest kostuda lasta signaalil. Kui mikrofon helisignaali kinni ei püüa, on kandidaat helianalüüsile vahele seganud.

Samuti võib taustaheli uurimine aimu anda teise arvuti abil toimuvast kommunikatsioonist. Kui sisseastumiseksami kaitsesüsteem analüüsib klahvivajutusi, saab trükkimisheli esinemisel, aga klahvivajutuste puudumisel järeldada, et ruumis on ka teine klaviatuuriga seade, mille kaudu on võimalik infot edastada ja seega eksamikorda rikkuda.

7 Ruumi pildianalüüs

Selleks, et takistada väljaspool kaamera vaatevälja olevate abivahendite kasutamist või kõrvaliste isikute viibimist ruumis, tuleks kandidaadil enne eksami algust lindistada 360-kraadine video ruumist, kus eksamit sooritatakse, kasutades selleks veebikaamerat. Oleks hea, kui tolleks hetkeks oleks võimalik luua ühendus inimesest järelevaatajaga, kes veenduks keskkonna sobilikkuses ja paluks vajadusel esemeid eemaldada, kuid kui see pole võimalik, tuleb eksaminandile koostada selge ja arusaadav juhend korrektse eksamikeskkonna ning lubatud materjalide ja seadmete kohta ning ruumist 360-kraadise ülevaate andev videoklipp hiljem üle vaadata.

Ruumi tuleks veebikaamera videopildi vahendusel analüüsida ka hiljem, eksami sooritamise ajal, veendumaks, et protsessi käigus ei lisandu ruumi inimesi. Selleks võib kasutada näotuvastust, jälgides lisaks esiplaanil oleva eksaminandi näole taustale tekkivaid näokujutisi, või liikumisanalüüsi, märgistades ohukohtadena kaadris toimuva lisaliikumise. Liikumise analüüs peaks olema võimalikult robustne ja pigem vähetundlik,

kuna vastasel juhul võib see iga eksaminandi toolis tahapoole nõjatumise märgistada kui taustaliikumise. Üks võimalus oleks siinkohal eeldada, et eksaminandi keha asub vahetult tema näo all [89], [111] ning analüüsida liikumist piirkonnas, mis ei ole märgistatud kui pea või keha ning loetakse seetõttu taustaks. Antud juhul võib süsteemi vallandada kasutaja ringutamine.

Veelgi rangema süsteemi puhul võiks kaaluda erinevate esemete, näiteks telefon, lisaarvuti, teksti sisaldavad plakatid, raamatud ja lehed, tuvastamist videopildist [33], kuid usutavasti ei ole see RangeForce sisseastumiseksami algversiooni jaoks äärmiselt vajalik lisafunktsioon ja võib süsteemi muuta asjatult tundlikuks.

8 Muu

Jälgides IP-aadresse, millelt sisseastumiseksamit lahendatakse, on võimalik välistada eksami lahendamise teenus [133]. Nimelt, kui sisseastumiseksamit lahendab ühelt ja samalt IP-aadressilt mitu erinevat kandidaati, võib tegemist olla juhtumiga, kus pakutakse teenust eksami sooritamiseks. Teisalt ei ole võimalik konkreetset IP-aadressi blokeerida, kuna tegemist võib olla ka situatsiooniga, kus kandidaadid lahendavad testi ühes ja samas avalikus internetipunktis, nagu näiteks raamatukogu, ülikool või ühiselamu. Korduvate IP-aadresside puhul saab kandidaadid märgistada ja testimistingimusi vestlusvoorus täpsustada.

Võimalik on analüüsida ka testi sooritamiseks kulunud aega. Kui see on liiga lühike, võis ülesanne olla varasemalt teada või läbi lahendatud. Liiga pikk aeg võib aga vihjata sellele, et testi lahendamist pikendas kellegi teisega konsulteerimine.

Huvitav kaitsemeede oleks kasutada „meepoti“ (*honey pot*) meetodit ehk koostada testi vastuseid või juhiseid sisaldav veebilehekülg, millele navigeerides tuvastatakse kasutaja võõrküpsiste (*third party cookie*) või IP-aadressi kaasabil, eeldusel, et meepoti-lehekülg avatakse samas seadmes, kus sooritatakse testi [20]. Loomulikult ei sisaldaks antud lehekülg tegelikult ühtegi vastust, kuid ülesande teksti muutmata kujul otsides kuvataks meepoti-lehekülg esimesena. Sellisel juhul on võimalik eristada kandidaate, kes üritavad leida ülesande samm-sammulist lahenduskäiku, nendest, kes kasutavad otsingut alamülesande probleemi lahendamiseks.

Lisa 3 – Kõnetuvastuse programmikood

```
var recognition = new (window.SpeechRecognition ||
                       window.webkitSpeechRecognition ||
                       window.mozSpeechRecognition ||
                       window.msSpeechRecognition)();
recognition.continuous = true;
var speaking = false;
recognition.start();

recognition.onspeechstart = function() {
    console.log(+new Date + ' Speaking started.');
    changeSpeakingStatus();
};

recognition.onspeechend = function () {
    console.log(+new Date + ' Speaking stopped.');
    recognition.stop();
    changeSpeakingStatus();
    setTimeout(function () {
        recognition.start();
    }, 1000);
};

function changeSpeakingStatus() {
    speaking = !speaking;
    $('#speakingStatus').text(speaking.valueOf());
}
```

Lisa 4 – Küberkaitse eriala sisseastumistesti jaoks sobiva süsteemi nõuded

Käesolevas lisas on esitatud peatükis 7 kirjeldatud Tallinna Tehnikaülikooli küberkaitse eriala sisseastumistesti funktsionaalsed ja mittefunktsionaalsed nõuded.

1 Funktsionaalsed nõuded

Eksamikorra rikkumise vastase kaitsesüsteemi funktsionaalsed nõuded on järgmised:

- Süsteem peab käivitudes paluma kasutaja autentimist. Kasutaja tuvastamiseks kasutatakse meiliaadressi, parooli ja näotuvastuse kombinatsiooni.
- Kui kasutajakontot süsteemi andmebaasis ei eksisteeri, peab süsteem võimaldama uut kasutajakontot luua.
- Kasutajakonto olemasolul peab süsteem võimaldama kasutajal sisse logida.
- Süsteem peab võimaldama välja logimist.
- Süsteem peab kasutajakonto loomisel salvestama kandidaadi meiliaadressi, ees- ja perekonnanime ning kandidaadi valitud salasõna.
- Süsteem peab kasutajakonto loomisel salvestama fotojäädvustuse kandidaadi pildiga isikut tõendavast dokumendist. Dokument võib olla süsteemi sisestatud kas sisse skannitud failina või kasutajakonto loomise ajal veebikaamera abil pildistades.
- Süsteem peab enne sisseastumistesti alustamist kandidaadile kuvama nimekirja testi tegemise ajal keelatud tegevustest.
- Süsteem peab enne iga sisseastumistesti sessiooni algust kandidaadilt nõudma ruumist ja töökohast 360-kraadist ülevaadet andva video lindistamist.

- Süsteem peab pärast sisse logimist ja ruumivideo lindistamist avama RangeForce keskkonna.
- Süsteem peab võimaldama RangeForce keskkonnas laborite sooritamist.
- Süsteem peab sisseastumistesti laborite sooritamise ajal salvestama veebikaamera videovoo, ruumiheli ja sisendseadmetelt (klaviatuur, hiir) saadava info.
- Süsteem peab laborite sooritamise ajal teostama kasutaja pidevtuvastust.
- Süsteem peab näotuvastust kasutades sisseastumistesti sooritamise ajal võrdlema registreerumisel salvestatud dokumendifotot veebikaamerast saadava videovooga kasutajast, tuvastamaks isikute vahetumist testi tegemise ajal. Kui veebikaamera videovoos esinev nägu erineb salvestatud dokumendifotol olevast näost, peab süsteem olukorra märgistama kui kehastusründe.
- Süsteem peab veebikaamerast saadavas videovoos tuvastama olukorra, kus kaamera vaateväljas on rohkem või vähem kui üks nägu. Kui nägusid videovoos ei ole, peab süsteem olukorra videolindistuses märgistama kui kandidaadi lahkumise soorituse ajal. Kui nägusid on videovoos rohkem kui üks, peab süsteem olukorra märgistama kui kõrvalise isiku viibimise ruumis.
- Süsteem peab veebikaamera videovoo abil tuvastama muutusi kasutaja näoilmes. Kui miimika erinevus keskendunud näoilmest on liiga suur, eriti kui kandidaat naeratab pidevalt, peab süsteem olukorra märgistama kui kõrvalise tegevusega tegelemise.
- Süsteem peab veebikaamera videovoo abil tuvastama muutusi kasutaja riiete värvis. Kui kasutaja keha ehk näo all olev ala muudab värvi, peab süsteem olukorra märgistama kui riiete värvi muutuse ja potentsiaalse kehastusründe.
- Süsteem peab veebikaamera videovoo abil jälgima kandidaadi silmade fookuspunkti ja pilgu liikumist. Kui pilgu liikumine ei ole vastavuses kursori liikumisega ekraanil, peab süsteem olukorra märgistama kui kehastusründe ja kõrvalise tegevusega tegelemise. Kui ekraanil kuvatakse tekstisisu, aga kandidaadi pilk ei liigu kordagi horisontaalsihis paremalt vasakule või teeb seda liiga vähe või mujal kui tekstisisu kuvamise kohal, peab süsteem olukorra

märgistama kui kehastusründe ja kõrvalise tegevusega tegelemise. Kui konkreetsesse ekraanipunkti liigutakse esmalt kursori ja seejärel pilguga, peab süsteem olukorra märgistama kui kehastusründe ja lisaekraani kasutamise.

- Süsteem peab analüüsima kandidaadi trükkimise dünaamikat. Kui trükkimisstiilis esineb märkimisväärseid kõrvalekaldeid kasutajaprofiili tavapärasest normist, peab süsteem olukorra märgistama kui kehastusründe.

- Süsteem peab analüüsima kandidaadi hiire kasutusviisi. Kui hiire kasutamise dünaamikas esineb märkimisväärseid kõrvalekaldeid kasutajaprofiili normist, peab süsteem olukorra märgistama kui kehastusründe.

- Süsteem peab tuvastama mikrofoni staatust, mängides kõlaritest helisignaali. Kui esitatud helisignaal mikrofoni sisendisse ei jõua, peab süsteem kasutajale kuvama hoiatuse ja takistama edasist tööd, kuni mikrofon ja kõlarid on sisse lülitatud.

- Süsteem peab ruumihelist tuvastama klaviatuuri klahvide vajutamise heli. Kui ruumihelis tuvastatakse klaviatuuri klahvide vajutamise heli, aga puudub klaviatuurisisend, peab süsteem olukorra märgistama kui potentsiaalse lisaseadme kasutamise.

- Süsteem peab ruumihelist tuvastama inimkõnet. Kui süsteem tuvastab ruumihelist inimkõne, peab süsteem olukorra märgistama kui kõrvalise isiku viibimise ruumis.

- Süsteem peab blokeerima teiste, kõrvaliste rakenduste avamist lokaalses masinas. Keelatud rakendused on näiteks ekraanijagamis- ja suhtlusprogrammid, brauserid, tekstitöötlusrakendused ja lokaalse masina faililehitseja.

- Süsteem peab blokeerima klaviatuuri klahvikombinatsioone kasutades ekraanipildi jäädvustamise.

- Süsteem peab blokeerima klaviatuuri klahvikombinatsioone kasutades teksti kopeerimise ja kleepimise.

- Süsteem peab blokeerima hiire paremkliki abil teksti kopeerimise ja kleepimise.

- Süsteem peab blokeerima klaviatuuri klahvikombinatsioone kasutades süsteemi peatamise või süsteemist väljumise.

- Süsteem peab tuvastama süsteemi käivitumise virtuaalmasinas ja sulguma, teavitades eelnevalt kasutajat sellest, et süsteemi ei ole lubatud käivitada virtuaalkeskkonnas.

- Süsteem peab tuvastama, mitu ekraani on ühendatud arvutiga, kus süsteem käivitati, ja kui neid on rohkem kui üks, peab süsteem sulguma, teavitades kasutajat sellest, et lubatud on ainult üks kuvariekraan.

- Süsteem peab siduma kasutajaprofiili RangeForce sisseastumistesti jooksul sooritatud labori virtuaalmasina logiga.

- Süsteem peab kasutajaprofiiliga seotud virtuaalmasina logist tuvastama eelnevalt ülikooli esindaja poolt keelatud rakenduste ja tegevuste nimekirja kantud programmide avamise ja tegevuste sooritamise ning märgistama taolise olukorra kui keelatud materjalide kasutamise.

- Süsteem peab eksamikorra rikkumist tuvastades langetama kandidaadi usalduskvooti.

Ülikooli esindaja jaoks mõeldud alamsüsteem ei tegele eelpool mainitud kaitsemeetmete rakendamise, vaid sisseastumiseksami administreerimisega, ja peab võimaldama järgmiste toimingute teostamist:

- RangeForce labori virtuaalmasinas keelatud rakenduste ja tegevuste nimekirja koostamine;

- kõigi sisseastumistesti sooritanud kandidaatide nimekirja vaatamine;

- üksikkandidaadi info vaatamine, sealhulgas skannitud või veebikaameraga pildistatud isikut tõendava dokumendi ja testi jooksul veebikaameraga tehtud lindistuse kaadrite võrdlemine;

- kandidaadi sooritusest tehtud salvestise vaatamine, sealhulgas testi algul ruumist ja töökohast 360-kraadise ülevaate andva video vaatamine;

- lindistuses märgistatud eksamikorra rikkumise kohtade manuaalne kontrollimine;
- süsteemi poolt kandidaadi sooritusele antava usalduskvoodi vaatamine ja kinnitamine või muutmine;

2 Mittefunktsionaalsed nõuded

Mittefunktsionaalsed nõuded süsteemile on alljärgnevad:

- Kaitsesüsteemi kasutusliideseks peab olema kandidaadi arvutisse installitud programm.
- Administreerimise alamsüsteemi kasutusliideseks peab olema veebirakendus.
- Süsteemi kasutajaliides peab olema eriala õppetöö keelest lähtudes vähemasti ingliskeelne.
- Süsteem ei tohi olla platvormispetsiifiline, see tähendab, et süsteem peab töötama kõigil enamlevinud operatsioonisüsteemidel, sealhulgas Microsoft Windows'il, Unix'il ja macOS'il.
- Süsteem peab töötama ilma eririistvarata, kasutades tööks ainult laua- või sülearvutit ja standardseid kergesti kätte saadavaid odavaid sisendseadmeid, nagu klaviatuur, hiir, veebikaamera, mikrofon, kõlarid.
- Süsteem peab andmete edastamiseks kasutama internetiühendust.
- Süsteem peab kasutaja pidevtuvastamiseks kasutama multimodaalseid meetodeid, st kombineerima näotuvastust, pilgu liikumise, trükkimisstiili ja hiire kasutuse analüüsi.
- Süsteemi peab olema võimalik täies mahus kasutada ka nägemist korrigeerivate vahenditega, nagu prillid või läätsed.
- Süsteemi peab olema laiendatav, st süsteemile peab olema hiljem võimalik lisada eksamikorra rikkumist tuvastavaid meetmeid, mida peab olema võimalik olemasolevatega kombineerida.

- Süsteem peab laborite sooritamise ajal kasutaja pidevtuvastamist teostama passiivselt, st ilma kasutajat segamata, veebikaamera ja sisendseadmete abil.
- Kasutaja pidevtuvastuses esinevad pausid ei tohi olla pikemad kui 5 sekundit, vältimaks kehastusründe toimumist.
- Süsteem ei tohi lõpetada tööd, kui tuvastab eksamikorra rikkumise esinemise.
- Süsteem ei tohi võimaldada ligipääsu kõrvalistele, autoriseerimata isikutele, tagamaks isiku- ja delikaatsete andmete kaitse.
- Süsteem ei tohi säilitada ebavajalikke isikuandmeid.
- Süsteem peab olema võimeline edukalt toimima ka siis, kui kasutaja biomeetrilised faktorid on muutunud.
- Süsteem peab klientarvuti ressursse kasutama ainult sellisel määral, mis on vajalik süsteemi elementaarseks tööks, kasutaja pidevtuvastuseks vajalike andmete kogumiseks ja nende edastamiseks serverile.